Научно-технический журнал

H&ES RESEARCH

Scientific and Technical Journal

НАУКОЕМКИЕ ТЕХНОЛОГИИ В КОСМИЧЕСКИХ ИССЛЕДОВАНИЯХ ЗЕМЛИ

HIGH TECHNOLOGIES IN EARTH SPACE RESEARCH

Журнал **H&ES Research** издается с 2009 года, освещает достижения и проблемы российских инфокоммуникаций, внедрение последних достижений отрасли в автоматизированных системах управления, развитие технологий в информационной безопасности, исследования космоса, развитие спутникового телевидения и навигации, исследование Арктики. Особое место в издании уделено результатам научных исследований молодых ученых в области создания новых средств и технологий космических исследований Земли.

Журнал H&ES Research входит в перечень изданий, публикации в которых учитываются Высшей аттестационной комиссиейРоссии (ВАК РФ), в систему российского индекса научного цитирования (РИНЦ), а также включен в Международный классификатор периодических изданий.

Тематика публикуемых статей в соответствии с перечнем группспециальностей научных работников по Номенклатуре специальностей:

- 05.11.00 Авиационная и ракетно-космическая техника
- 05.12.00 Радиотехника и связь
- 05.13.00 Информатика, вычислительная техника и управление.

H&ES Research is published since 2009. The journal covers achievements and problems of the Russian infocommunication, introduction of the last achievements of branch in automated control systems, development of technologies in information security, space researches, development of satellite television and navigation, research of the Arctic. The special place in the edition is given to results of scientific researches of young scientists in the field of creation of new means and technologies of space researches of Earth.

The journal H&ES Research is included in the list of scientific publications, recommended Higher Attestation Commission Russian Ministry of Education for the publication of scientific works, which reflect the basic scientific content of candidate and doctoral theses. IF of the Russian Science Citation Index.

Subject of published articles according to the list of branches of science and groups of scientific specialties in accordance with the Nomenclature of specialties:

- 05.07.00 Aviation, space-rocket hardware
- 05.12.00 RF technology and communication
- 05.13.00 Informatics, computer engineering and control.

ИНДЕКСИРОВАНИЕ ЖУРНАЛА H&ES RESEARCH

JOURNAL H&ES RESEARCH INDEXING

• NEICON • CyberLenika (Open Science) • Google Scholar • OCLC WorldCat • Ulrich's Periodicals Directory • • Bielefeld Academic Search Engine (BASE) • eLIBRARY.RU • Registry of Open Access Repositories (ROAR)

Все номера журнала находятся в свободном доступе на сайте журнала **www.hes.ru** и библиотеке **elibrary.ru.**

Всем авторам, желающим разместить научную статью в журнале, необходимо оформить ее согласно требованиям и направить материалы на электронную почту: **HT-ESResearch@yandex.ru.**
С требованиями можно ознакомиться на сайте: **www.H-ES.ru.**

Язык публикаций: русский, английский.
Периодичность выхода – 6 номеров в год.
Свидетельство о регистрации СМИ ПИ № ФС 77-60899 от 02.03.2015
Территория распространения: Российская Федерация, зарубежные страны

Тираж 1000 экз. Цена 1000 руб.
Плата с аспирантов за публикацию рукописи не взимается.

All issues of the journal are in a free access on a site of the journal **www.hes.ru** and **elibrary.ru.**

All authors wishing to post a scientific article in the journal, you must register it according to the requirements and send the materials to your email: **HT-ESResearch@yandex.ru.**
The requirements are available on the website: **www.H-ES.ru.**

Language of publications: Russian, English.
Periodicity – 6 issues per year.
Media Registration Certificate PI No. FS77-60899. Date of issue: March 2, 2015.
Distribution Territory: Russian Federation, foreign countries

Circulation of 1000 copies. Price of 1000 Rur.
Postgraduate students for publication
of the manuscript will not be charged

3 2021 Т. 13

ISSN 2409-5419 (Print) ISSN 2412-1363 (Online) WWW.H-ES.RU Дата выхода: 25 июня 2021

Учредитель:
ООО «ИД Медиа Паблишер»

Издатель:
ДЫМКОВА С.С.

Главный редактор:
ЛЕГКОВ К.Е.

Адрес издателя:
111024, Россия, Москва, ул. Авиамоторная, д. 8, офис 512-514.

Адрес редакции:
194044, Россия, Санкт-Петербург, Лесной Проспект, 34-36, к. 1,
Тел.: +7(911) 194-12-42.

Адрес типографии:
Россия, Москва, ул. Складочная, д. 3, кор. 6.

СОДЕРЖАНИЕ

РАДИОТЕХНИКА И СВЯЗЬ

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

CONTENTS

RF TECHNOLOGY AND COMMUNICATION

INFORMATICS, COMPUTER ENGINEERING AND CONTROL

Founder:
"Media Publisher", LLC

Publisher:
DYMKOVA S.S.

Editor in chief:
LEGKOV K.E.

Address of publisher:
111024, Russia, Moscow, st. Aviamotornaya, 8, office 512-514;

Address of edition:
194044, Russia, St. Petersburg, Lesnoy av., 34-36, h.1,
Phone: +7 (911) 194-12-42.

Address of printing house:
Russia, Moscow, st. Skladochnaya, 3, h. 6

Doi: 10.36724/2409-5419-2021-13-3-4-18

МЕТОДИКА КОНТРОЛЯ И ПРОГНОЗИРОВАНИЯ ТЕХНИЧЕСКОГО СОСТОЯНИЯ СИСТЕМЫ ВТОРИЧНОГО ЭЛЕКТРОПИТАНИЯ ПОЛЕВЫХ ОБЪЕКТОВ СВЯЗИ НА ОСНОВЕ НЕЙРОСЕТЕВОГО ПОХОДА

АБРАМКИН
Роман Викторович[1]

ПЕДАН
Алексей Викторович[2]

ВИНОГРАДЕНКО
Алексей Михайлович[3]

АННОТАЦИЯ

Введение: в настоящее время контроль технического состояния сложных технических систем, таких как, система вторичного электропитания полевых объектов связи, представляет собой длительный и неавтоматизированный процесс, который осуществляется операторами непосредственно на самих объектах контроля. Данное обстоятельство оказывает негативное влияние на своевременность выявления отказов контролируемого объекта. Также, весьма негативным фактором является полное отсутствие какого-либо прогноза технического состояния объекта контроля, что приводит к внезапным отключениям вторичной системы электропитания полевых объектов связи, и, соответственно, перерыву связи. Совокупность данных факторов крайне отрицательно сказывается как на устойчивой работе системы связи в целом, так и на коэффициенте исправного действия направления связи, в частности. **Цель работы** заключается в разработке методик контроля и прогнозирования технического состояния системы вторичного электропитания полевых объектов связи. **Используемые методы:** применение нейросетевого подхода позволяет добиться весьма точных результатов и получить высокое быстродействие систем в режиме реального времени. **Новизна работы** заключается в повышении точности и скорости контроля, возможности прогнозирования технического состояния, интеграции системы вторичного электропитания в информационную среду полевого объекта связи путем применения нейросетевых технологий. **Результат:** применение нейросетевого подхода позволяет осуществлять прогнозирование технического состояния, а также более точно классифицировать техническое состояние объекта контроля. Также, появляется возможность централизации контроля, что, в свою очередь, позволяет снизить время контроля. **Практическая значимость:** результаты работы можно использовать в процессе контроля и прогнозирования технического состояния сложных технических систем, что позволит значительно снизить количество аварийных ситуаций.

КЛЮЧЕВЫЕ СЛОВА: контроль технического состояния; прогнозирование; нейронная сеть; система вторичного электропитания; обучающая выборка; класс технического состояния; объект контроля.

Сведения об авторах:

[1]адъюнкт Военной академии связи им. С.М. Буденного, г. Санкт-Петербург, Россия, avg62rus@rambler.ru

[2]к.т.н., старший преподаватель Военной академии связи им. С.М. Буденного, Санкт-Петербург, Россия, cepberok@gmail.com

[3]к.т.н., доцент, докторант Военной академии связи имени Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия, vinogradenko.a@inbox.ru

Для цитирования: *Абрамкин Р.В., Педан А.В., Виноградeнко А.М.* Методика контроля и прогнозирования технического состояния системы вторичного электропитания полевых объектов связи на основе нейросетевого похода // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13. № 3. С. 4–18. Doi: 10.36724/2409-5419-2021-13-3-4-18

Введение

Анализ современных систем контроля технического состояния системы вторичного электропитания (СВЭП) полевых объектов связи (ПОС) свидетельствует о том, что существует объективная научно-техническая проблема создания комплексных систем контроля, построенных на универсальных принципах, обеспечивающих высокий уровень достоверности контроля и прогнозирования технического состояния изделий при заданной оперативности.

Важнейшим условием эффективной работы СВЭП ПОС является необходимость контроля текущего технического состояния элементов самой системы и прогнозирования их поведения в течение дальнейшей эксплуатации.

Контроль позволяет оценить текущее состояние СВЭП ПОС и существенно сократить время на поиск и устранение неисправностей, а прогнозирование — определить время наступления отказа и предотвратить его, что может значительно повысить надежность оборудования. По своей сути, задачу контроля и прогнозирования технического состояния СВЭП ПОС можно свести к задаче наблюдения за величинами диагностических признаков выбранных каналов диагностирования.

Аналитические методики контроля технического состояния определяют, выделяют и классифицируют отказы в компонентах системы. Основной проблемой разработки аналитических моделей контроля является определение разности. Большинство определителей разности основаны на моделях линейных систем. Для нелинейных систем основным подходом является их линеаризация. Однако, для систем с высокой степенью нелинейности и большим количеством нелинейных операций, такая линеаризация не дает удовлетворительных результатов. Единственным решением данной проблемы является использование большого количества линейных систем, что не очень практично при создании моделей, работающих в реальном времени. Процесс создания моделей очень сложен и точность получаемых результатов проверить затруднительно. В условиях, когда решение задачи аналитически в общем виде не представляется возможным, применим нейросетевой подход, обеспечивающий достаточно высокое качество ее выполнения [1].

Возможность нейронных сетей (НС) моделировать сложные системы обладая небольшим количеством информации, позволяет использовать их в аналитических моделях.

Причины, послужившие применению НС в задачах контроля и прогнозирования:

– для реализации нейросетевых алгоритмов необходима минимальная информация об объекте;

– при реализации НС возможна параллельная обработка информации, что позволяет значительно увеличить скорость работы системы;

– задачи прогнозирования отказов изделий сложны из-за невозможности четкой постановки соответствия изменений входных и выходных параметров состояния, в котором находится или к которому стремится объект контроля;

– при реализации НС возможно проводить обслуживание и текущий ремонт изделия по фактическому текущему техническому состоянию, что обеспечит рациональный расход ресурсов [2].

Основные направления применения НС в СВЭП ПОС:

1. Применение НС для параметрического диагностирования.

Данное направление основано на сравнении математической модели конкретного СВЭП ПОС с моделью бездефектного элемента, т.е. в проверке принадлежности параметров состояний допустимым диапазонам их рассеивания (область профилактических допусков и граничные значения). Выход параметра за пределы этих диапазонов (рис. 1) должен свидетельствовать о наличии неисправности СВЭП ПОС. В настоящее время для обнаружения отказов в контролируемых объектах используется интервальный метод, суть которого состоит в задании допустимого интервала значений выходной величины каждого

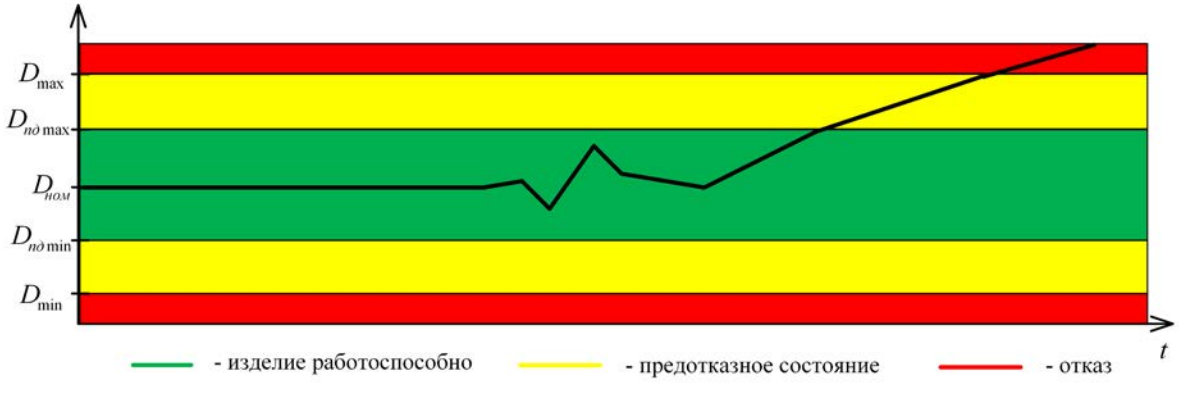


Рис. 1. Аппроксимированная кривая изменения значения контролируемого параметра на фоне областей, классифицирующих техническое состояние объекта контроля

контролируемого параметра (рабочего диапазона). При выходе этой величины за пределы рабочего диапазона принимается решение об отказе контролируемого элемента.

Состояние любой СВЭП ПОС характеризуется большим количеством параметров, значения которых можно получить, используя штатные средства измерения, или же путем проведения дополнительных испытаний на работающем или отключенном электрооборудовании.

Область значений контролируемого параметра, характеризующая переход объекта контроля в предотказное состояние обуславливается введением профилактических допусков. Такой подход позволяет более точно определять класс технического состояния, и своевременно осуществлять маневры оборудованием, не допуская перерыва связи из-за отказа СВЭП ПОС.

2. Применение НС для прогнозирования технического состояния СВЭП ПОС.

НС на основе разработанной определенной методики позволяет строить зависимость одного параметра от другого в виде полинома. То есть, она может позволить найти скрытые зависимости, одной величины от другой, которые невозможно определить методами прямых измерений. В свою очередь, прогнозирование значений контролируемых параметров позволяет осуществить прогнозирование технического состояния СВЭП ПОС на конкретном временном интервале с заданной вероятностью. Точность прогноза зависит от обучающей выборки, количества слоев НС, вида связей между слоями, выбора функции активации, а также от ряда других факторов [3].

Экспериментальная оценка методик контроля и прогнозирования технического состояния осуществлялась для СВЭП ПОС, включающей в себя блок ВС (ввод силовой), блок БКК (блок коммутации каналов), блок ВУ (выпрямительное устройство), блок ЦРУ (центральное распределительное устройство), блок ЩРПТ (щит распределительный постоянного тока), блок ЩРПрТ (щит распределительный переменного тока), инвертор, блок автоматики (БА) (рис. 2).

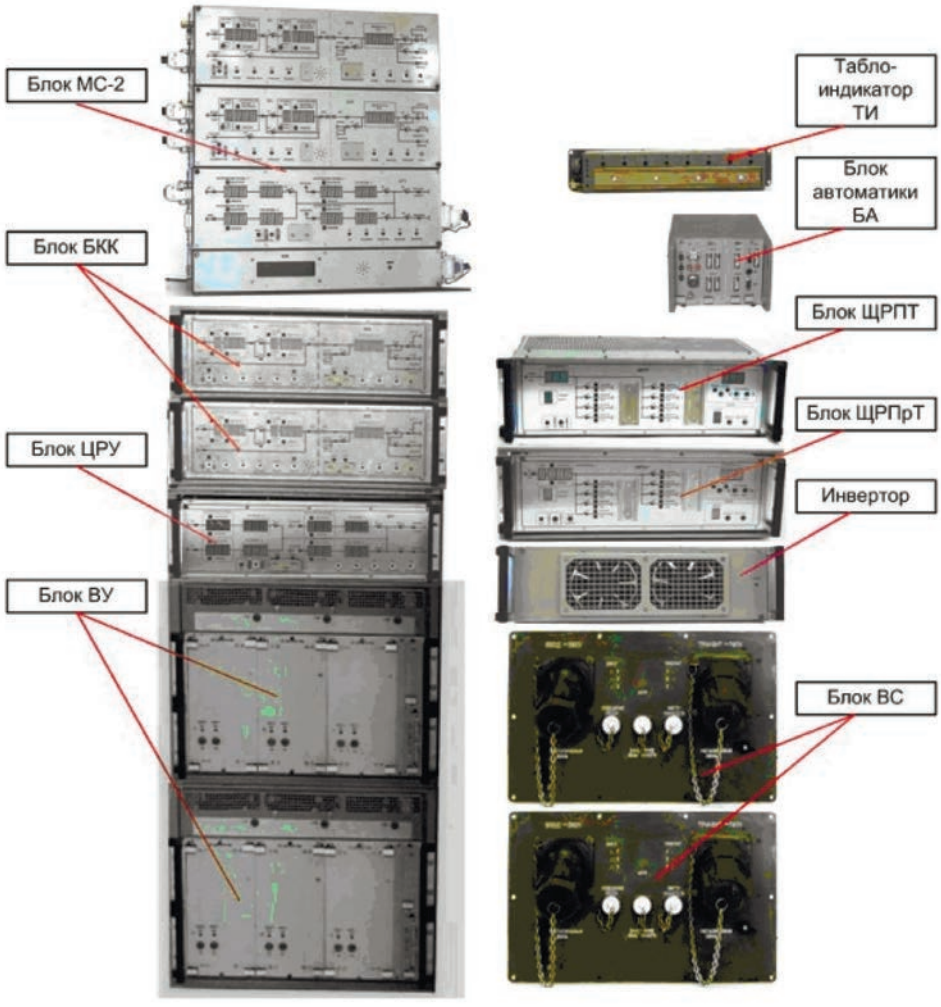


Рис. 2. Система вторичного электропитания подвижных объектов управления и связи

Применение нейронных сетей в системе контроля и прогнозирования технического состояния СВЭП ПОС

На рис. 3 представлен обобщенный подход к использованию нейронных сетей в рамках решения задач контроля и прогнозирования технического состояния СВЭП ПОС.

Основная суть заключается в формировании классов текущего и прогнозного технического состояния и их графическом представлении оператору с целью реализации своевременных управленческих решений по недопущению перерывов связи из-за неисправностей СВЭП ПОС.

Для этого необходима реализация 4-х классов технического состояния для текущего контроля СВЭП ПОС (работоспособно, предотказ, регулировка первичного источника питания (ПИП), отказ) и 3-х классов для прогнозирования (работоспособно, предотказ, отказ).

Класс технического состояния «Требуется регулировка ПИП», представляет собой класс, схожий по значениям параметров с предотказным состоянием, но имеющим иную природу возникновения. Он определяется критическими параметрами качества электрической энергии, поступающей от первичного источника питания. В случае появления данного класса технического состояния предполагается, что будет оказано управляющее воздействие на первичный источник питания по регулированию его параметров в норму (формирование на экране лица принимающего решения (ЛПР) сообщения «Необходима регулировка ПИП» будет свидетельствовать не об отказе СВЭП, а лишь о необходимости регулировки параметров ПИП в норму).

Благодаря данному подходу, становится возможным разграничение предотказного состояния, возникшего по причине внутренней неисправности СВЭП и состояния, при котором произошел выход контролируемых параметров за пределы допусков в результате внешнего дестабилизирующего воздействия. То есть, можно сделать вывод о повышении достоверности контроля.

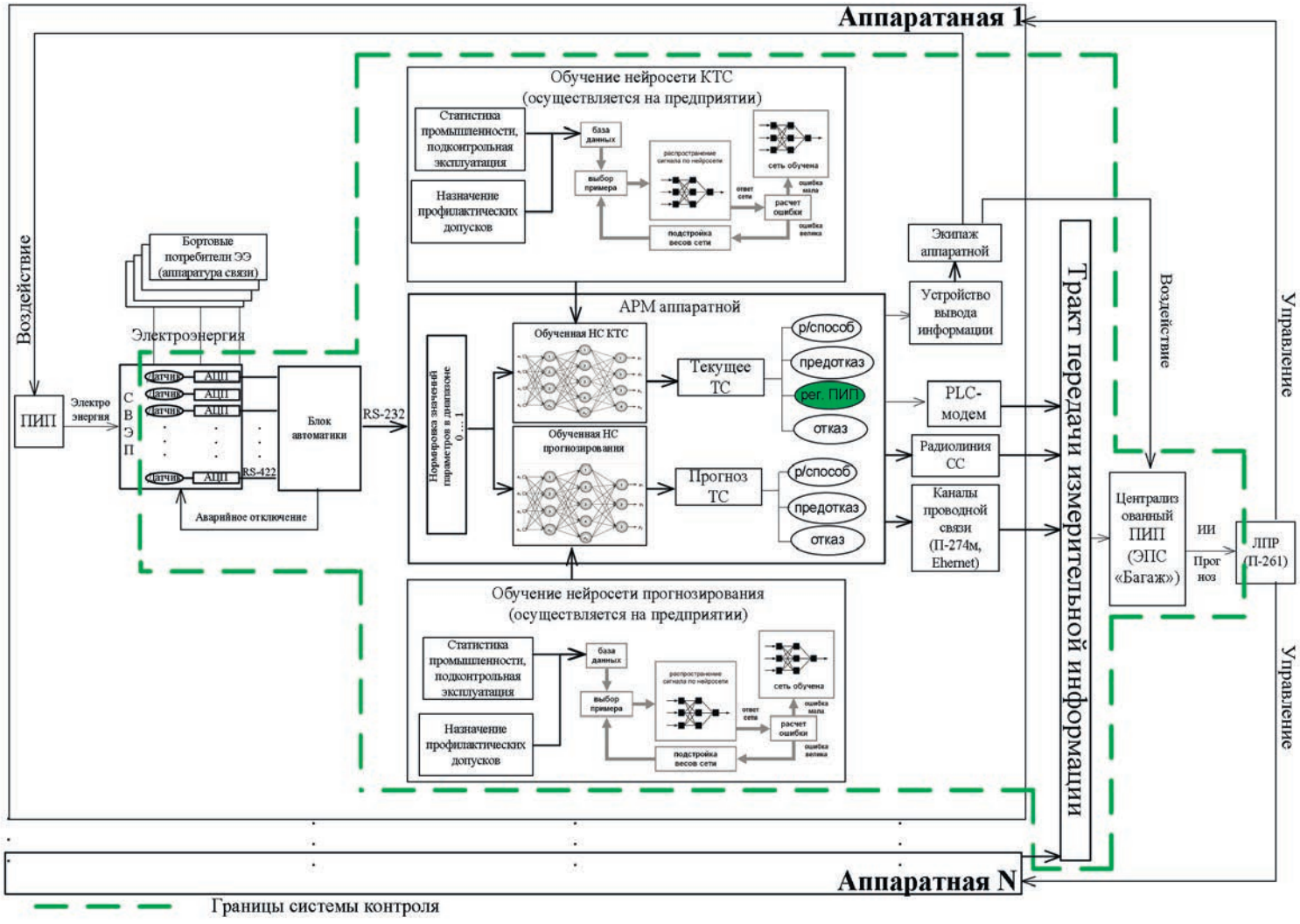


Рис. 3. Структурная схема контроля и прогнозирования технического состояния СВЭП ПОС системы связи командного пункта группировки войск (сил)

Выбор инструмента контроля и прогнозирования технического состояния СВЭП ПОС

Основной целью является определение класса технического состояния СВЭП ПОС в зависимости от входных данных (значений контролируемых параметров), то есть, решение задачи классификации. Оно представляет собой совокупность методов, позволяющих классифицировать многомерные наблюдения, каждый из которых описывается набором характеристик — в данном случае это может быть набором сигналов с различных датчиков СВЭП ПОС. Имея на входе рассматриваемой методики определенную совокупность значений показателей, можно однозначно интерпретировать ее выходные значения как оценку технического состояния СВЭП ПОС.

Применение нейросетей контроля и прогнозирования технического состояния позволяет проводить классификацию состояния СВЭП ПОС, то есть отнести его состояние к одному из классов состояний, определяемых по данному виду испытаний или измерений.

Однако, высокая динамика и нелинейность процессов, а также сложность структурных связей, определяют необходимость использования для оценки состояния средства, имеющие высокую адаптивность и устойчивость к внешним шумам.

Не смотря на явные преимущества и широкие возможности нейронных сетей, исследования показывают, что в большинстве случаев их применение как элементов систем контроля весьма ограничено.

В работах [4, 5] рассматриваются вопросы реализации экспертных и самообучающихся систем, базирующихся на алгоритмах нечеткой логики и гибридных нейронных сетях. Основным недостатком предложенных решений является необходимость в существенных временных, интеллектуальных и вычислительных затратах, что в нашем случае нецелесообразно, т. к. будут использоваться и без того невысокие вычислительные мощности штатных автоматизированных рабочих мест (АРМ) аппаратных связи.

В работах [6–9] предлагаются системы в которых используются методики гибридных нейронных сетей. Для функционирования этих достаточно простых в реализации систем не требуются значительные вычислительные ресурсы. Однако, общим их недостатком является отсутствие возможности прогнозирования и ограниченные возможности по интерпретации полученных результатов.

В статье [10] предлагается подход к прогнозированию на основе комбинирования вероятностной и обычной многослойной нейронных сетей. Комбинирование нейронных сетей различных типов позволяет существенно уменьшить время на обучение нейросетевой системы, однако недостатком этого подхода является низкая устойчивость к воздействию шумов на исходные данные.

Полученные в работах [11, 12] результаты по реализации динамических эволюционных систем с нечеткой логикой позволяют производить адаптивное обучение в режиме времени, приближенном к реальному, и прогнозировать тенденции изменения входных параметров системы с течением времени. Однако для оценки состояния СВЭП ПОС такой подход достаточно сложен и не всегда приемлем.

Таким образом, релевантные работы показывают, что с учетом необходимой точности классификации и прогнозирования, а также сильной ограниченности в вычислительных ресурсах, решение поставленной задачи контроля и прогнозирования вполне достижимо путем применения нейронных сетей прямого действия, а именно, многослойного персептрона (однонаправленной НС).

Реализация методик контроля и прогнозирования технического состояния СВЭП ПОС

Изначальными процедурами построения однонаправленной сети являются задание топологии и правил обучения. Топология выбирается исходя из требуемой точности идентификации, содержания задачи, количества параметров процесса, размерности вектора входных данных. Настройка сети представляет собой многоходовой итерационный процесс, при котором периодически анализируются результаты и регулируются параметры: количество слоев, количество нейронов в слое, выбор функции активации. Нейронные сети не требуют традиционного программирования: информация обучения НС накапливается в весах, а не в программах. Это делает их устойчивыми к флуктуациям входных воздействий и обеспечивает устойчивость работоспособности сети при выходе из строя отдельных ее компонент. На возникший дефект сеть реагирует только изменением качества функционирования при сохранении общей работоспособности.

Увеличение количества слоев позволяет выявить более тонкие статистические закономерности. Однако, размерность сети должна соответствовать размерности данных обучающей выборки. В противном случае, способность сети к обучению будет снижаться, или наоборот, будет утрачена способность сети определять основные параметры отображения.

Количество нейронов входного (сенсорного) слоя определяется количеством контролируемых параметров технического состояния СВЭП ПОС, а выходного слоя — количеством классов технического состояния. Теоретически определено, что для аппроксимации заданного преобразования вполне достаточно не более двухтрех скрытых слоев ИНС с не более чем (2N+1) количеством нейронов в каждом скрытом слое [13].

На рис. 4 и 5 представлен общий вид НС контроля текущего технического состояния СВЭП ПОС и НС прогнозирования.

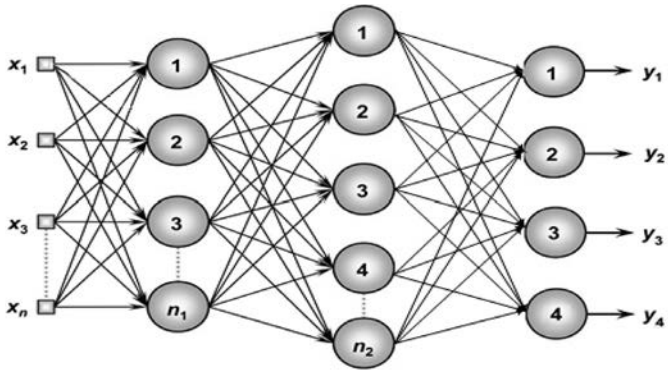


Рис. 4. Общий вид разработанной НС контроля технического состояния СВЭП ПОС

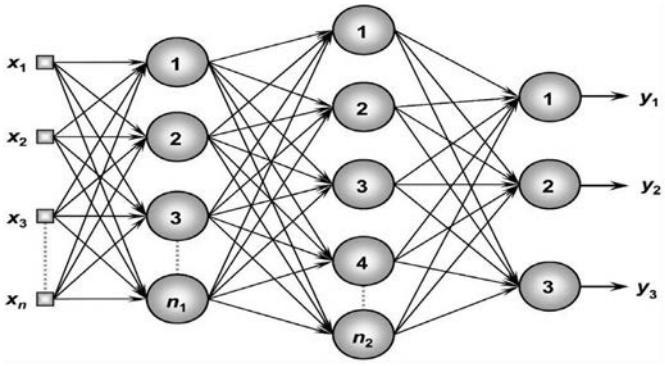


Рис. 5. Общий вид разработанной НС прогнозирования технического состояния СВЭП ПОС

Методика контроля текущего технического состояния СВЭП ПОС реализована на основе использования многослойного персептрона (рис. 4). В качестве вектора входных данных (X_1, X_2, …, X_n) выступают значения показателей, полученные с датчиков СВЭП ПОС. Обучающей выборкой является статистическая информация, полученная в результате заводских испытаний на предприятии промышленности контролируемых СВЭП ПОС, а также данные подконтрольной эксплуатации изделий. Методика предполагает обработку нормированных значений контролируемых параметров (нормирование осуществляется в диапазоне от 0 до 1), поступающих на вход НС и выделение целевого класса, определяющего текущее техническое состояние СВЭП ПОС. Целесообразность применения данной НС определяется тем, что она имеет простую структуру и легко обучается, не теряя при этом в точности выходных данных, а также требует минимальных вычислительных ресурсов для своей работы.

Применение многослойного персептрона возможно не только с целью определения текущего класса технического состояния, но и для его последующего прогнозирования. Главным отличием от НС контроля текущего технического состояния является обучающая выборка, а также измененная структура самой сети (количество нейронов выходного слоя) (рис. 5). В результате, по совокупности значений показателей на выходе прогнозирующей НС можно однозначно интерпретировать прогнозируемое техническое состояние СВЭП через заданный промежуток времени.

При использовании нейросетевых методов существуют различные способы выделения областей технического состояния. В настоящее время применяются различные способы реализации запоминания областей. Наиболее используемые из них — это выделение областей гиперплоскостями и покрытие областей гипершарами. Для запоминания одной из ограничивающих область гиперплоскости достаточно сохранения n+1 значения, где n — размерность пространства. Соответственно, для запоминания одного гипершара также требуется j значение: координаты центра и радиус [14].

В нейронных сетях для запоминания каждой гиперплоскости или гипершара используется отдельный элементарный вычислитель — нейрон, а для запоминания всех гиперплоскостей или гипершаров используется объединение составляющих нейронов в параллельную структуру — нейросеть. Как показывают исследования, выделение области работоспособности и областей отказа и предотказа в двумерном пространстве основных диагностических признаков наиболее целесообразно проводить гиперплоскостями.

Совокупность гиперплоскостей представляется объединением нейронов в нейросеть, выполняющую параллельную согласованную работу всех нейронов, что обеспечивает оперативное решение задачи идентификации точки области, выделяемой при построении сети. Каждый нейрон j задает значениями весов своих входов уравнение гиперплоскости:

$$a_j = \sum_{i=0}^{n(j)} W_{ji} X_{ji} = 0, \qquad (1)$$

где $n(j)$ — количество входов нейрона j, a_j — величина порога функции активации, $j \in 1,2 \ldots N$, обеспечивает оперативное решение задачи об идентификации точки области, выделяемой при построении сетей. НС способна аппроксимировать любую непрерывную функцию, определенную на ограниченном множестве $\{x_1, x_n\}$ с любой заданной точностью $\varepsilon > 0$:

$$f(x_1 \ldots x_n) = \sum_{i=1}^{N} V_i \left(\frac{1}{1 + e^{-\sum_{i=1}^{n(j)} W_i^j X_i^j}} \right), \qquad (2)$$

где N — количество нейронов первого слоя; W_i^j — вес j-го входа i-го нейрона первого слоя с сигмоидальной функцией активации, $i = 1, N; j = 1, n$.

Во многих исследованиях аналогичных задач описывается применение карты Кохонена, где в ходе ее самообучения выстраивается алгоритм, при котором после каждого этапа ее работы происходит оценка Евклидовой меры

между «центрами» полученных классов. Центром каждого класса технического состояния является среднее арифметическое соответствующих примеров данного класса. Если Евклидово расстояние слишком мало — данные классы объединяются и алгоритм обучения продолжается.

Однако, поскольку представленные нейросети обучаются на основании имеющейся статистической выборки, а при обучении каждому набору входных данных указывается свой, соответствующий этим данным класс технического состояния, то фактически осуществляется обучение сети с учителем. К тому же, на основании статистических наблюдений и испытаний были выявлены значения для каждого контролируемого параметра, после превышения которых, состояние объекта контроля характеризовалось повышенным риском отказа. Исходя из этого, были определены профилактические допуски для каждого контролируемого параметра. Соответственно, при формировании обучающей выборки на основании статистических наблюдений, каждому набору входных данных был присвоен соответствующий класс технического состояния. Поэтому, применение карты Кохонена для определения количества классов технического состояния объекта контроля в данном случае не обязательно, а учитывая и без того малые вычислительные ресурсы имеющихся АРМ полевых объектов связи — нецелесообразно [15–16].

Таким образом, объем и точность обучающей выборки, равно как и введение профилактических допусков, позволяют обойтись без данных усложнений методики.

Исследования проводились следующим образом. Методом экспертных оценок была определена группа наиболее важных параметров СВЭП ПОС, значения которых необходимо контролировать. В результате заводских испытаний на предприятии промышленности и данных подконтрольной эксплуатации была получена статистика по каждому из контролируемых параметров, достаточная для корректного обучения нейронных сетей. После этого, структура методики строилась в соответствии с конфигурацией СВЭП и, соответственно, количеством контролируемых параметров с последующим обучением искусственных нейронных сетей. Выходам каждой НС задавалось определенное число классов, каждый из которых соответствовал определенному, строго заданному техническому состоянию СВЭП: работоспособен, предотказное состояние, отказ для НС контроля, и работоспособен, предотказ, необходима регулировка ПИП, отказ для НС прогнозирования соответственно.

В качестве функции активации в нейронах каждого слоя осуществлялся экспериментальный выбор между сигмоидальной функцией (1) и ReLU (2) (рис. 6).

$$\sigma(x) = \frac{1}{1+e^{-x}} \tag{3}$$

$$\max(0, x) \tag{4}$$

$$\sigma(x) = \frac{1}{1+e^{-x}}, \max(0, x) \tag{5}$$

Формирование и обучение нейронных сетей осуществлялось в программной среде AnyLogic. В ходе проведения исследований было выявлено, что при использовании функции ReLU обучение нейросетей осуществлялось дольше, а ошибка обучения была больше. (рис. 7, 8).

На примере рис. 8 видно, что, при использовании сигмоидальной функции активации при одинаковом количестве обучающих тактов, ошибка составляет 6,9%, что на 2,2% меньше, чем при использовании функции ReLU. По результатам данного эксперимента в качестве функции активации нейронов в каждом слое была выбрана сигмоидальная функция. Аналогичная картина наблюдалась и при обучении прогнозной нейронной сети (рис. 8).

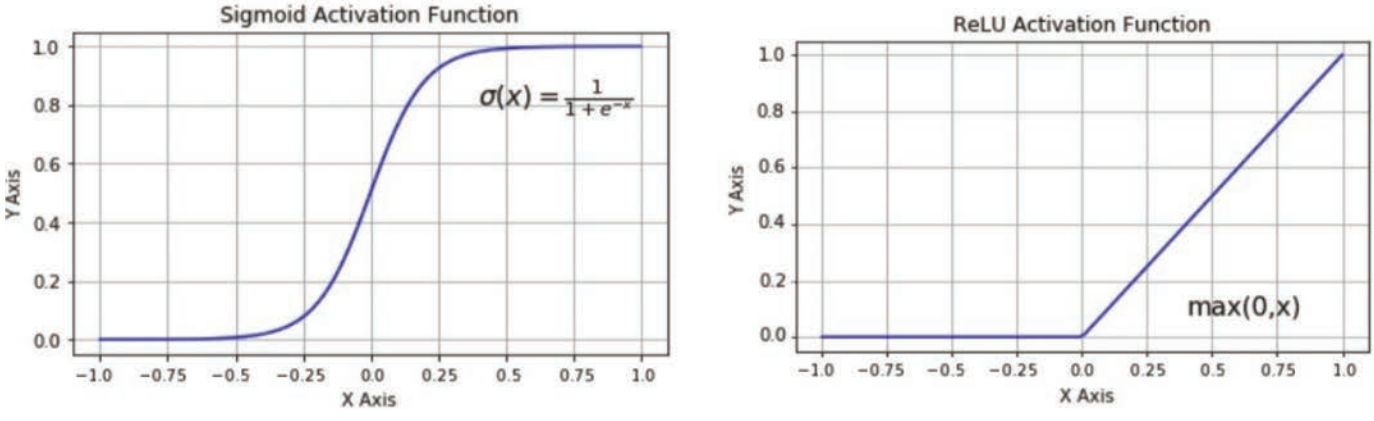


Рис. 6. Сигмоидальная функция активации и ReLU

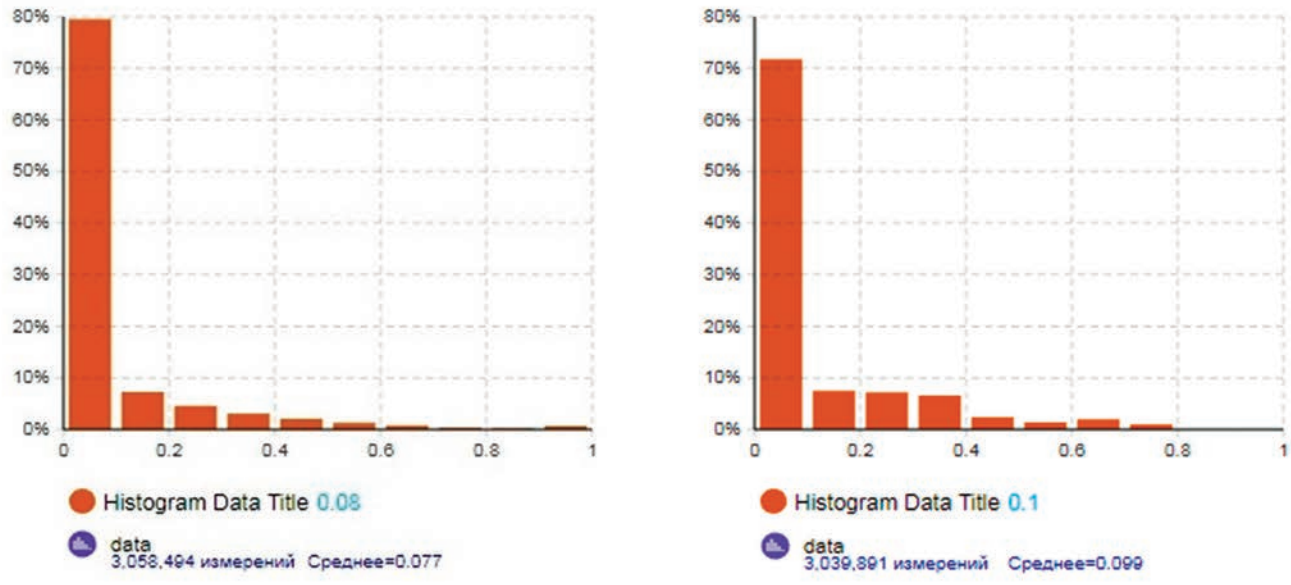


Рис. 7. Гистограммы ошибок при использовании сигмоидальной функции и ReLU для НС прогнозирования

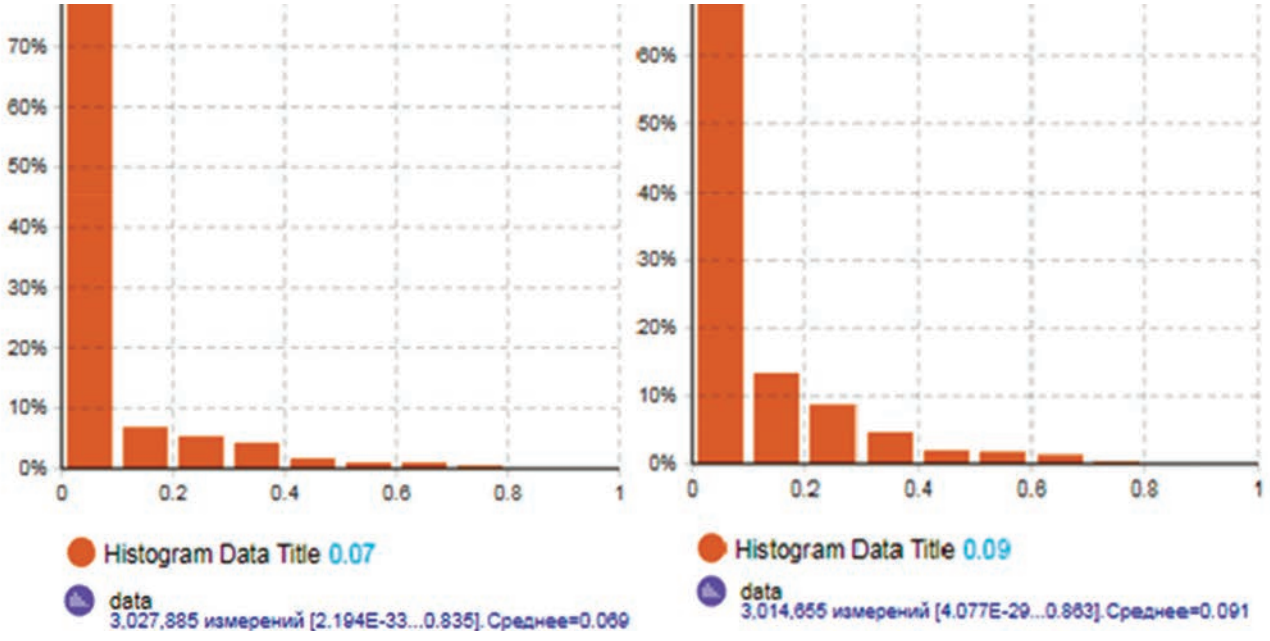


Рис. 8. Гистограммы ошибок при использовании сигмоидальной функции и ReLU для НС контроля текущего технического состояния

Данный факт объясняется тем, что при использовании функции ReLU при достижении отрицательных значений аргумента функции активации, ее производная становится равной нулю и дальнейшее обучение становится нецелесообразным, так как полученная ошибка меняться не будет.

В ходе решении вопроса обучения НС необходимо найти минимум функции ошибки, то есть минимизировать следующее выражение:

$$E = \sum_{k=1}^{L} E(k) = \frac{1}{2\sum_{k=1}^{L} (y^k - t^k)^2}, \quad (6)$$

где $E(k)$ — среднеквадратичная ошибка сети; y^k и t^k — выходное и эталонное значения НС для k-го примера вектора измеряемых параметров.

Выполнение данной задачи не тривиально, так как данная функция является сложной и многомерной (рис. 9), из-за чего ее математическая обработка сопряжена с большими трудностями. Для поиска минимума функции ошибки в рассматриваемых НС применялся метод градиентного спуска. Его применение оправдано в случае функции многих переменных, когда другие методы не обеспечивают требуемых результатов, либо их невозможно реализовать на практике. Также, он устойчив к наличию дефектных данных и не приводит далеко в неправильную сторону, даже если время от времени совершаются неверные шаги поиска минимума.

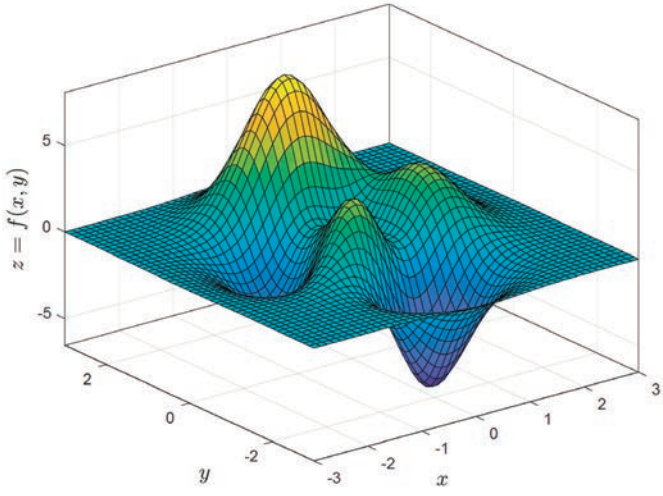


Рис. 9. Общий вид многомерной поверхности ошибки

Для уменьшения величины ошибки НС, то есть для минимизации среднеквадратического отклонения текущих выходных значений сигнала от устанавливаемых в многослойной нейронной сети, необходима корректировка весовых коэффициентов синаптических связей между нейронами. С целью решения данной задачи использовался алгоритм обратного распространения ошибки (backpropagation). Данный алгоритм является первым и основным практически применимым для обучения многослойных нейронных сетей, особенно в рамках решения задачи классификации. При использовании алгоритма обратного распространения, сигнал ошибки на выходе НС распространяется в направлении, обратном выходу с последующей корректировкой синаптических весов нейронной сети для достижения минимальной выходной погрешности.

В ходе работы была рассмотрена возможность использования «отложенного» обучения НС, при котором ошибка копится пока не будут поданы все обучающие векторы на вход НС в отличии от стандартного алгоритма обратного распространения, когда веса модифицируются непосредственно после предъявления каждого обучающего вектора и возможно «забывание» векторов выборки, предъявленных ранее. То есть, все входные данные обрабатываются сетью, ошибки вычисляются, производится обратное распространение, но изменения весов не производятся, они накапливаются, и модификация делается после прохождения всей обучающей выборки (веса обновляются только после предъявления сети всей обучающей выборки). Главным достоинством данного метода является отсутствие необходимости предъявлять образцы в случайном порядке, то есть обучение НС осуществляется в процессе штатной эксплуатации оборудования. Однако, нейросети, используемые в СВЭП ПОС, уже должны быть обучены и готовы к определению/прогнозированию технического состояния. Также, данный метод не всегда обеспечивает быструю сходимость [17]. С учетом особенностей работы системы контроля СВЭП, связанных с высокой достоверностью и оперативностью, был выбран классический алгоритм обратного распространения ошибки.

Веса синаптических связей нейронной сети образуют матрицу весов связей β:

$$\beta = \begin{pmatrix} w_{11}\ w_{21} \dots w_{n1} \\ w_{12}\ w_{22} \dots w_{n2} \\ \vdots \quad \vdots \quad \ddots \quad \vdots \\ w_{1m}\ w_{2m} \dots w_{nm} \end{pmatrix}, \qquad (7)$$

где $w_{11} \dots w_{nm}$ — веса связей между нейронами. Выходное значение каждого нейрона каждого слоя (за исключением сенсорного) является результатом работы функции активации. Связи между нейронами всех слоев являются всеобъемлющими (полносвязная сеть) с подстройкой весов синаптических связей на обучающей стадии. Каждый выходной сигнал *b*-го слоя подается на вход всех нейронов (*b*+1)-го слоя. Математически выход *i*-го нейрона (*b*+1)-го слоя можно представить в следующем виде:

$$y_i^{b+1} = \sum_{s=1}^{M_b} w_{is}^{b+1} y_s^b + w_{s0}^{b+1},\ i = 1 \dots M_{b+1}, \qquad (8)$$

где w_{is}^{b+1} — вес связи *s*-го нейрона (*b*+1)-го слоя с *i*-м нейроном *b*-го слоя; w_{s0}^{b+1} — величина внешнего смещения. Результат адаптивного суммирования (сумма произведений выходных значений нейронов предыдущего слоя на значения весовых коэффициентов связей с этим нейроном) является аргументом функции активации, посредством которой выполняется преобразование входных воздействий в выходной сигнал с настраиваемыми характеристиками. Настройка (обучение) сетей предусматривает процедуру регулирования весовых коэффициентов входов нейронов и приведение к нулю порога аргумента функции активации. Обучение нейросети состоит из тактов и эпох. Каждый такт обучения *k*-й эпохи соответствует одновременной подаче

на вход сети сигнала входа эмпирической выборки и сравнении сигнала выхода эмпирической выборки с выходным сигналом НС. В каждом такте обучения персептрон взаимодействует с одной из пар векторов вход — выход. После реализации всего объема выборки данных вход — выход *k*-я эпоха обучения заканчивается и оценивается значение суммарной выходной среднеквадратической ошибки E_k НС с матрицей весовых коэффициентов (9).

$$E_k = \|Y - X\| / n, \tag{9}$$

где Y — истинный вектор обучающей выборки, X — результат нейросетевой обработки, n — количество нейронов выходного слоя.

В общем виде выход НС можно описать выражением (10):

$$O^k = \frac{1}{1 + e^{-w^T o^k}}, \tag{10}$$

где w — вектор весов выходного слоя, o^k — вектор выходов нейронов скрытого слоя с элементами. Для его определения используется выражение (11):

$$o^k = \frac{1}{1 + e^{-w_i^T x^k}}, \tag{11}$$

где w_i — вектор весов, связанных с i-м скрытым нейроном; $i = 1 \ldots n$.

Градиентная корректировка весов выполняется на основе минимизации квадратичной функции ошибки с помощью выражений:

$$W = W - \eta[\partial E_k(W, w) / \partial W], \tag{12}$$

$$w_i = W - \eta[\partial E_k(W, w) / \partial w_i], \tag{13}$$

где $\eta = const$ — коэффициент скорости обучения, $\eta \in (0,1)$. Для сигмоидальной функции активации выражение примет вид (14):

$$\partial E_k(W, w) / \partial W = \frac{1}{2} \frac{\partial}{\partial W (y^k - \frac{1}{1 + e^{-w^T o^k}})^2} = \\ = -(y^k - O^k) O^k (1 - O^k) o^k. \tag{14}$$

В результате, в скалярной форме получается выражение (15):

$$W_i := W_i + \eta \delta_k o_i^k \tag{15}$$

где δ_k описывается выражением (16):

$$\delta_k = (y^k - O^k) O^k (1 - O^k) \tag{16}$$

В скалярной форме выражение для корректировки весов синаптических связей нейронной сети примет вид (17):

$$w_{ij} = w_{ij} + \eta \delta_k W_i o_i^k (1 - o_i^k) x_j^k \tag{17}$$

Второе слагаемое выражения (17) представляет собой произведение скорости обучения, разницы между значениями нейрона выходного слоя и истинного вектора обучающей выборки, производной активационной функции и значения функции, соответствующему j-му весу.

Коэффициент скорости обучения НС η изначально полагается равным 0,6 ($0<\eta<1$) и затем постепенно уменьшается в процессе обучения. Это позволяет делать большие начальные шаги для быстрого грубого обучения, и меньшие шаги при подходе к окончательной величине.

На рис. 10 в общем виде представлен алгоритм обучения нейросетей контроля и прогнозирования технического состояния СВЭП ПОС.

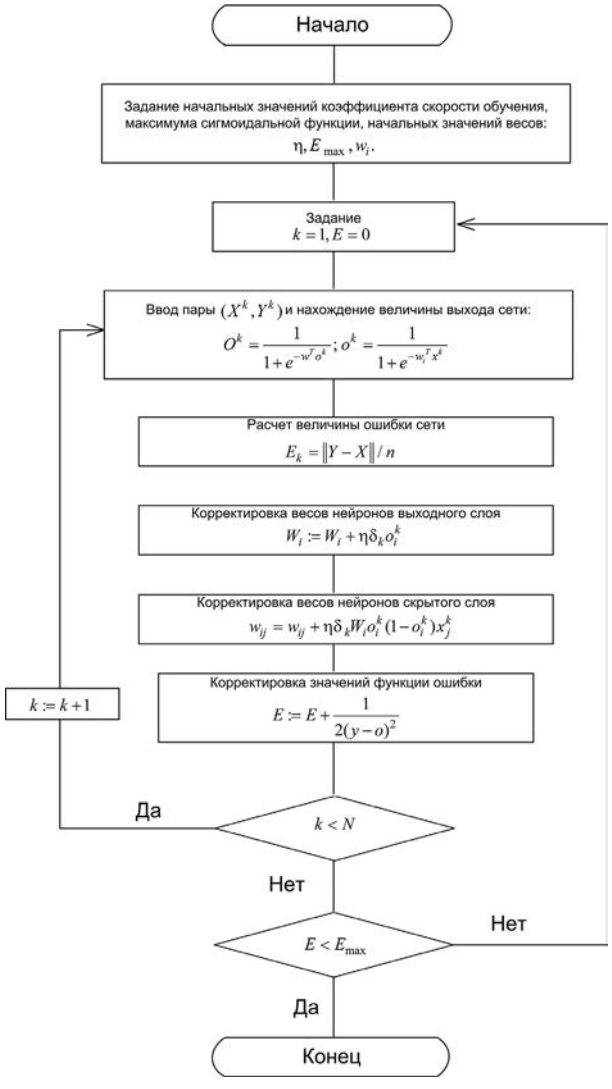


Рис. 10. Алгоритм обучения нейросетей контроля и прогнозирования технического состояния СВЭП ПОС

Обученные НС обладают способностью обобщения, т.е. имеют возможность давать статистически корректный ответ на входные сигналы, принадлежащие классу обучающих данных, но не использующиеся ни при обучении, ни при тестировании.

Количество нейронов скрытых слоев выбиралось исходя из относительной простоты поставленной задачи, а также невысоких вычислительных мощностей АРМ ПОС. Кроме того, немаловажными аспектами являются исключение переобучения НС, снижение ошибки и увеличение скорости обучения.

По завершении обучения, искусственные нейронные сети контроля и прогнозирования технического состояния СВЭП ПОС, полностью готовы к дальнейшей эксплуатации.

Топология таких сетей характеризуется тем, что количество нейронов в выходном слое, как правило, равно количеству определяемых классов. При этом, устанавливается соответствие между выходом нейронной сети и классом, который он представляет. Когда сети предъявляется некий образ (набор значений параметров), на одном из её выходов должен появиться признак того, что образ принадлежит этому классу. В то же время на других выходах должен быть признак того, что образ данному классу не принадлежит. Если на двух или более выходах есть признак принадлежности к классу, считается что сеть «не уверена» в своём ответе.

В задачах классификации выходной элемент должен выдавать «сильный» сигнал в случае, если данное наблюдение принадлежит к интересующему нас классу, и «слабый» — в противоположном случае. Иначе говоря, выходом обученной нейросети является кодовая последовательность, соответствующая своему классу технического состояния [18–19].

На выходе каждого нейрона выходного слоя формируется числовое значение в диапазоне (0;1) (т.к. применяется сигмоидальная активационная функция). Кодовое значение «1» присваивается выходному нейрону, значение которого наибольшее. Всем остальным выходным нейронам присваивается кодовое значение «0». Таким образом, обученная нейросеть прогнозирования может выдавать следующие коды классов состояний: «100», «010», «001», что соответствует работоспособному состоянию, предотказному состоянию и отказу. Для НС контроля текущего технического состояния предусмотрены следующие коды классов: «1000»; «0100»; «0010»; «0001», что соответствует работоспособному состоянию, предотказному состоянию, состоянию, при котором необходима регулировка ПИП, отказу. На начальном этапе обучения значения нейронов выходного слоя примерно одинаковы, как это показано на рис. 10 (0,424; 0,365; 0,406 для НС прогнозирования и 0,369; 0,365; 0,508; 0,464 для НС контроля текущего технического состояния) и «перевес» значений является минимальным, а ошибка, соотвественно, весьма большая. Однако, значению 0,424 (для НС прогнозирования) будет присвоен код «1», а остальным — «0». Соответственно, выходом нейросети в данном случае будет являться кодовая последовательность «100», что соответствует работоспособному прогнозному состоянию объекта контроля. Аналогичная ситуация наблюдается для НС контроля текущего технического состояния СВЭП ПОС. Значению 0,508 будет присвоен код «1», а остальным — «0». Соответственно, выходом нейросети в данном случае будет являться кодовая последовательность «0010», что соответствует состоянию объекта, при котором необходима регулировка ПИП. В ходе дальнейшего обучения НС данный «перевес» по выходам нейронов выходного слоя становится максимальным, и, соответственно, уменьшается ошибка НС.

После обучения НС, разница значений нейронов выходного слоя составляет от одного до нескольких порядков, благодаря чему ошибка становится минимальной (рис. 11, 12).

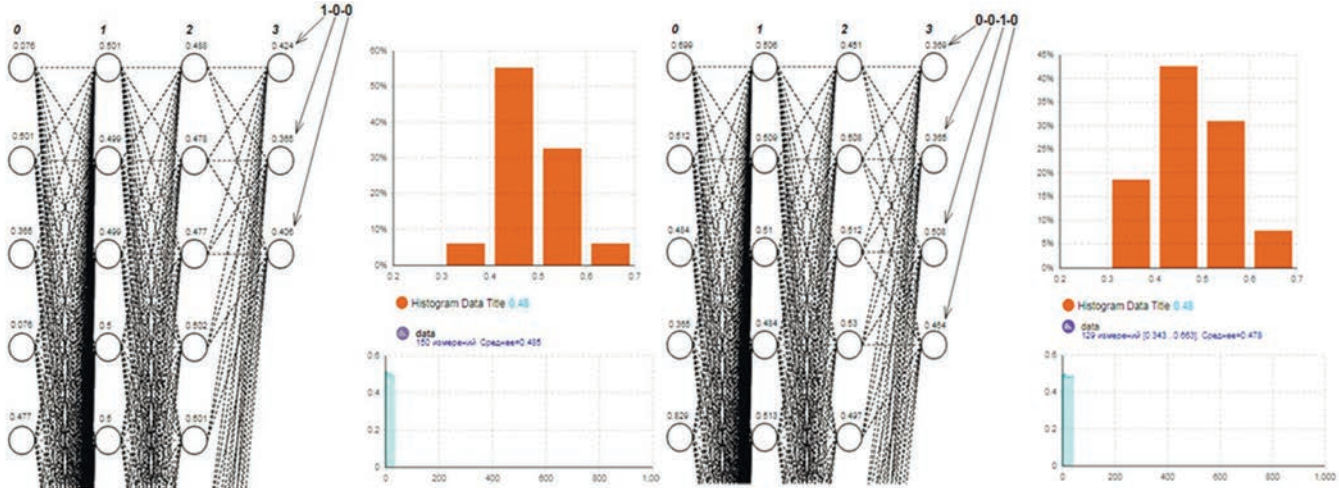


Рис. 11. Состояние НС прогнозирования и контроля технического состояния на начальном этапе обучения

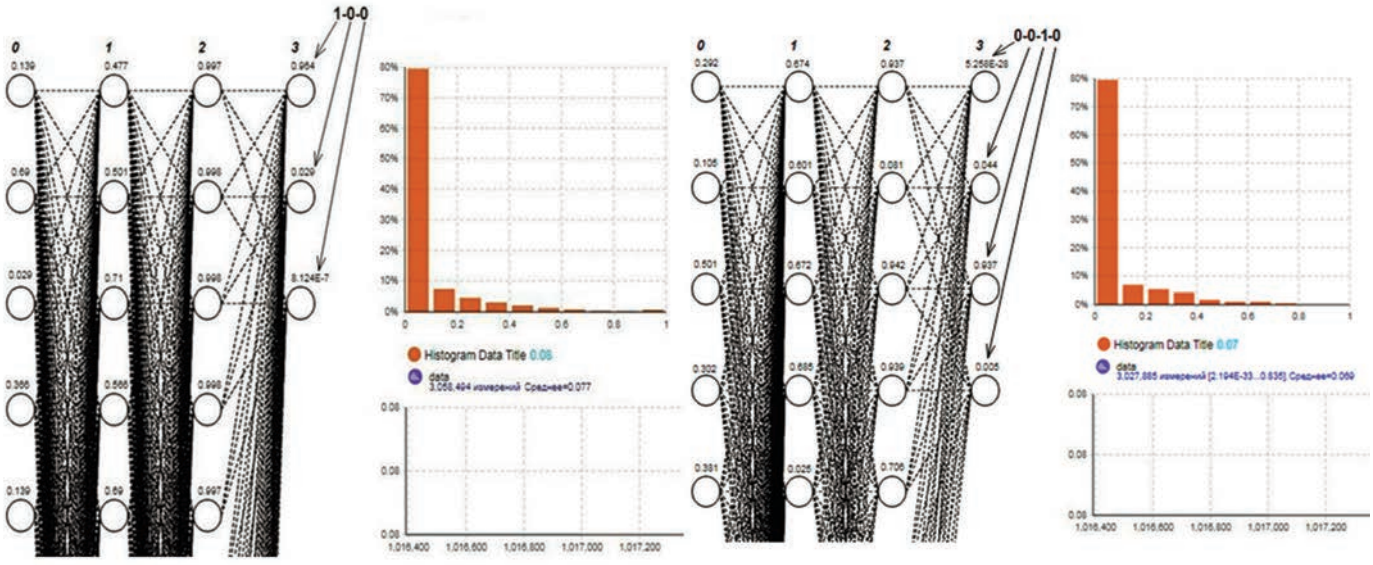


Рис. 12. Состояние обученных НС контроля и прогнозирования технического состояния

Применение метода окон в задаче прогнозирования технического состояния СВЭП ПОС

По сути, можно сказать, что задача прогнозирования на нейронных сетях формализуется через задачу распознавания образов. Данные о прогнозируемой переменной за некоторый промежуток времени образуют образ, класс которого определяется значением прогнозируемой переменной в некоторый момент времени за пределами данного промежутка, т.е. значением переменной через интервал прогнозирования. Использование метода окон предполагает использование двух окон W_i и W_o с фиксированными размерами. Эти окна, способны перемещаться с некоторым шагом по временной последовательности исторических данных, начиная с первого элемента, и предназначены для доступа к данным временного ряда, причем первое окно W_i, получив такие данные, передает их на вход нейронной сети, а второе — W_o — на выход. Получающаяся на каждом шаге пара используется как элемент обучающей выборки (распознаваемый образ, или наблюдение). Временная последовательность исторических данных представляет собой статистические выборки значений контролируемых параметров и коды классов технического состояния [20].

Каждый следующий вектор получается в результате сдвига окон W_i и W_o вправо на один элемент.

Нейронная сеть, обучаясь на этих наблюдениях и соответственно настраивая свои коэффициенты, извлекает эти закономерности и формирует прогноз.

Обученная прогнозирующая НС способна выдавать информацию в режиме реального времени о возможном техническом состоянии объекта контроля через заданный временной интервал. Поскольку НС представляет собой дискретную систему, то настройка «плавности» срока прогнозирования весьма затруднительна, так как в полной мере будет определяться обучающей выборкой. Например, НС, осуществляющая прогнозирование на интервал, равный 10 минутам не способна без дополнительных манипуляций осуществить прогноз на другой интервал, так как она была обучена осуществлять прогнозирование именно через этот временной промежуток. Такая особенность НС привносит определенные сложности в работу системы контроля и прогнозирования технического состояния, поскольку в начале работы системы появляется интервал времени, в течении которого определяется только текущее техническое состояние объекта контроля без его прогнозирования (например, с момента включения оборудования до наступления момента времени первого прогноза) (рис. 13). Длительность данного интервала определяется величиной периода прогнозирования прогнозной НС.

Рис. 13. Общий вид временного интервала работы объекта контроля и НС

На данном рисунке $t_{вкл}$ представляет собой время включения оборудования (СВЭП ПОС); $t_{НС}$ — время наступления первого прогноза НС; $t_{выкл}$ — время выключения оборудования.

С целью исключения негативного влияния данного обстоятельства, предлагается ввести вспомогательные прогнозные НС, интервалы прогнозирования которых полностью перекроют интервал времени, в течении которого определяется только текущее техническое состояние объекта контроля без его прогнозирования. Включение вспомогательных НС будут осуществляться поочередно, замещая друг друга, что позволит реализовать данную систему на штатных АРМ аппаратных связи без изыскания дополнительных вычислительных ресурсов. Обучающие выборки вспомогательных прогнозных НС формируются индивидуально для каждой в зависимости от интервала прогнозирования.

Экспериментальная оценка достоверности и эффективности предложенных методик

После обучения НС, на их входы были поданы тестовые выборки значений контролируемых параметров. Данные выборки являлись статистическими данными, полученными в результате испытаний. Фильтрация выборок осуществлялась таким образом, чтобы в их множестве находились все классы технического состояния объекта контроля. Основной момент заключается в том, что данные значения не участвовали в обучении НС, и, соответственно их можно приравнять к значениям, получаемых НС с выходов датчиков контролируемых параметров. Результаты воздействия 520 тестовых выборок представлены в табл. 1 и 2.

Таблица 1

Результаты проверки работы НС контроля технического состояния

Класс технического состояния	НС контроля технического состояния	
	Число тестов	ошибка, %
Работоспособен	230	6,8
Предотказ	117	6,1
Регулировка ПИП	121	6,2
Отказ	52	5,9

Таблица 2

Результаты проверки работы НС прогнозирования технического состояния

Класс технического состояния	НС прогнозирования технического состояния	
	Число тестов	ошибка, %
Работоспособен	233	7,7
Предотказ	194	6,8
Отказ	93	6,3

Как видно из таблиц, предложенные методики контроля и прогнозирования технического состояния СВЭП ПОС обеспечивают высокую достоверность на этапе принятия решения.

Результаты экспериментальных исследований показали, что простота структуры и минимальные требования к используемым вычислительным ресурсам говорят о том, что представленные методики могут успешно применяться в системах контроля СВЭП ПОС.

Заключение

Проведенные эксперименты и исследования подтвердили целесообразность использования нейросетей для решения задач контроля и прогнозирования технического состояния. Это дает возможность внедрения новейших компьютерных технологий в производство комплексов, применяемых на объектах контроля. Применение НС дает возможность решить задачу классификации областей состояний объекта контроля.

Таким образом, активное внедрение нейросетевых технологий в процесс контроля и прогнозирования технического состояния позволяет взглянуть на это совершенно по-другому и открывает новые горизонты возможностей в данной области исследований.

Литература

1. *Саенко И.Б., Скорик Ф.А., Котенко И.В.* Мониторинг и прогнозирование состояния компьютерных сетей на основе применения гибридных нейронных сетей // Изв. ВУЗов. Приборостроение. 2016. Т. 59. № 10. С. 795–800.

2. *Kotenko I., Saenko I., Skorik F., Bushuev S.* Neural network approach to forecast the state of internet of things elements // Proc. of the XVIII Intern. Conf. on Soft and Computer and Measurements, IEEE Xplore. 2016. Pp. 140–148.

3. *Виноградеико А.М.* Прогнозирование отказов контролируемых комплексов связи специального назначения // Системы управления, связи и безопасности. 2020. № 3. С. 222–237.

4. *Zhang, Y., Wang Y., Wu L.* Research on Demand-driven Leagile Supply Chain Operation Model: A Simulation Based on AnyLogic in System Engineering // Systems Engineering Procedia. 2018. Vol. 3. Pp. 249–258.

5. *Souza L.G. M., Baretto G.A.* Nonlinear system identification using local arx models based on self-organizing map. Learning and Nonlinear Models // Revista da Sociedade Brasiliera de Redes Neurais (SBRN). 2016. Vol. 4. No. 2. Pp. 112–123.

6. *Budko, P.A., Fedorenko V.V., Vinogradenko A.M., Samoylenko V.V., Pedan A.V.* Approach to the intellectual monitoring of the technical condition of difficult dynamic objects on the basis of the systems of a polling // Distributed computer and communication networks: control, computation, communications Springer, Cham. 2019. Vol. 1141. Pp. 560–573.

7. *Azruddin A., Gobithasan R., Rahmat B., Azman S., Sureswaran R.* A hybrid rule based fuzzy-neural expert system for passive network monitoring // Proc. of the Arab Conf. on Information Technology ACIT. 2016. Pp. 746–752.

8. *Fedorenko V.V., Kononov Y.G, Samoylenko V.V., Zelensky E.G.* Development of a distributed multi-agent system monitoring and control

networks of 0.4–35 kV // In: Proceedings of the 2017 IEEE Intern. Conf. on Control in Technical Systems (CTS) (2017). Pp. 271–274.

9. *Mishra A., Zaheeruddin Z.* Design of hybrid fuzzy neural network for function approximation // J. of Intelligent Learning Systems and Applications. 2018. Vol. 2. No. 2. Pp. 97–109.

10. *Викторова Е.В.* Применение нечетких нейронных сетей для технической диагностики дорожных машин // Вестник ХНАДУ. 2018. Вып. 56. С. 98–102.

11. *Kumar S., Lokeshab M., Manjunath L.H.* A Review on Automatic Fault Detection and Diagnosis in a Single Point Cutting Tool Using Wavelet Analysis // International Journal of Advances in Scientific Research and Engineering. 2017. No. 3(1). Pp. 230–234.

12. *Simoens P., Dragone M., Saffiotti A.* The Internet of Robotic Things: A review of concept, added value and applications // International Journal of Advanced Robotic Systems I–II. 2018. Pp. 1–9.

13. *Горева Т.И., Порнягин Н.Н., Пюкке Г.А.* Нейросетевые модели диагностики технических систем // Вестник КРАУНЦ. Физ-мат. науки. 2017. № 1 (4). С. 31–43.

14. *Виноградено А.М., Заяц С.В., Кузнецов С.В.* Перспективы развития полевых и стационарных средств технического обеспечения // Материалы III ВНПК «Современные проблемы создания и эксплуатации ВВСТ». Санкт-Петербург, 2016. Т. 2. С. 157–161.

15. *Zołtowski M., Martinod R.* Technical Condition Assessment of Masonry Structural Components using Frequency Response Function (FRF) // Journal of the International Masonry Society Masonry International. 2016. Vol. 29(1). Pp. 23–27.

16. *Хаханов В.И., Щерба О.В.* Применение искусственных нейронных сетей для диагностирования цифровых сетей // Радиоэлектронные и компьютерные системы. 2017. № 5 (46). С. 15–20.

17. *Антонюк Е.М., Ломоносова Ю.С.* Системы автоматического контроля со сжатием данных // Известия СПбГЭТУ (ЛЭТИ). 2017. № 7. С. 62–68.

18. *Климов В.В., Крапивин В.Ф., Мкртчян Ф.А., Ничипор А.Е.* Методы классификации и качественной интерпретации данных дистанционного мониторинга окружающей среды // Экологические системы и приборы. 2019. № 3. С. 7–12.

19. *Волобуев М.Ф., Уфаев В.А.* Обнаружение постепенных отказов в резервированной измерительной системе в зависимости от полноты вероятностного описания выходных сигналов // Информационно-измерительные и управляющие системы. 2017. Т. 15. № 10. С. 28–35.

20. *Волобуев М.Ф., Мальцев А.М., Михайленко С.Б., Уфаев В.А.* Способ обнаружения отказов при экономичном резервировании бортового оборудования беспилотного летательного аппарата // Журнал Сибирского федерального университета. Техника и технологии. 2016. № 9 (7). С. 1060–1067.

METHODOLOGY FOR MONITORING AND PREDICTING THE TECHNICAL CONDITION OF THE SECONDARY POWER SUPPLY SYSTEM OF FIELD COMMUNICATION OBJECTS BASED ON A NEURAL NETWORK CAMPAIGN

ROMAN V. ABRAMKIN
St. Petersburg, Russia, avg62rus@rambler.ru

ALEXEY V. PEDAN
St. Petersburg, Russia, cepberok@gmail.com

ALEKSEY M. VINOGRADENKO,
St. Petersburg, Russia, vinogradenko.a@inbox.ru

KEYWORDS: technical condition monitoring; forecasting; neural network; secondary power supply system; training sample; tchnical condition class; control object.

ABSTRACT

Introduction: currently, the control of the technical condition of complex technical systems, such as the secondary power supply system of field communication facilities, is a long and non-automated process that is carried out by operators directly at the control facilities themselves. This circumstance has a negative impact on the timely detection of failures of the controlled object. Also, a very negative factor is the complete absence of any forecast of the technical condition of the control object, which leads to sudden disconnections of the secondary power supply system of field communication facilities, and, accordingly, a break in communication. The combination of these factors has an extremely negative effect both on the stable operation of the communication system as a whole, and on the coefficient of serviceable operation of the communication direction, in particular. **The purpose of the work** is to develop methods for monitoring and predicting the technical condition of the secondary power supply system of field communication facilities. **Methods used:** the application of the neural network approach allows you to achieve very accurate results and get high performance systems in real time. **The novelty of the work** is to increase the accuracy and speed of control, the ability to predict the technical condition, the integration of the secondary power supply system into the information environment of the field communication object by using neural network technologies. **Result:** the application of the neural network approach allows you to predict the technical condition, as well as

more accurately classify the technical condition of the control object. Also, it becomes possible to centralize control, which, in turn, reduces the control time. **Practical significance:** the results of the work can be used in the process of monitoring and predicting the technical condition of complex technical systems, which will significantly reduce the number of accidents.

REFERENCES

1. Saenko I.B., Skorik F.A., Kotenko I.V. Monitoring i prognozirovanie sostoyaniya komp'yuternyh setej na osnove primeneniya gibridnyh nejronnyh setej [Monitoring and forecasting of the state of computer networks based on the use of hybrid neural networks]. *Izv. VUZov. Priborostroenie* **[**Journal of Instrument Engineering**].** 2016. Vol. 59. No. 10. Pp. 795–800. (In Rus)

2. Kotenko I., Saenko I., Skorik F., Bushuev S. Neural network approach to forecast the state of internet of things elements. *Proc. of the XVIII Intern. Conf. on Soft and Computer and Measurements*, IEEE Xplore. 2016. Pp. 133–135.

3. Vinogradenko A.M. Prognozirovanie otkazov kontroliruemyh kompleksov svyazi special'nogo naznacheniya [Forecasting failures of controlled communication complexes for special purposes]. *Sistemy upravleniya, svyazi i bezopasnosti* [Control systems, communications and security]. 2020. No. 3. Pp. 222–237. (In Rus)

4. Zhang, Y., Wang Y., Wu L. Research on Demand-driven Leagile Supply Chain Operation Model: A Simulation Based on AnyLogic in System Engineering. *Systems Engineering Procedia.* 2018. Vol. 3. Pp. 249–258.

5. Souza L.G. M., Baretto G.A. Nonlinear system identification using local arx models based on self-organizing map. Learning and Nonlinear Models. *Revista da Sociedade Brasiliera de Redes Neurais (SBRN).* 2016. Vol. 4. No. 2. Pp. 112–123.

6. Budko, P.A., Fedorenko V.V., Vinogradenko A.M., Samoylenko V.V., Pedan A.V. Approach to the intellectual monitoring of the technical condition of difficult dynamic objects on the basis of the systems of a polling. *Distributed computer and communication networks: control, computation, communications.* Springer, Cham. 2019. Vol. 1141. Pp. 560–573.

7. Azruddin A., Gobithasan R., Rahmat B., Azman S., Sureswaran R. A hybrid rule based fuzzy-neural expert system for passive network monitoring. *Proc. of the Arab Conf. on Information Technology ACIT.* 2016. Pp. 746–752.

8. Fedorenko V.V., Kononov Y.G, Samoylenko V.V., Zelensky E.G. Development of a distributed multi-agent system monitoring and control networks of 0.4–35 kV. *Proceedings of the 2017 IEEE Intern. Conf. on Control in Technical Systems (CTS) (2017).* Pp. 271–274. (In English)

9. Mishra A., Zaheeruddin Z. Design of hybrid fuzzy neural network for function approximation. *J. of Intelligent Learning Systems and Applications*. 2018. Vol. 2. No. 2. Pp. 97–109.

10. Viktorova E.V. Primenenie nechetkih nejronnyh setej dlya tekhnicheskoj diagnostiki dorozhnyh mashin [Application of fuzzy neural networks for technical diagnostics of road machines]. *Vestnik HNADU* **[**]. 2018. Vol. 56. Pp. 98–102. (In Rus)

11. Kumar S., Lokeshab M., Manjunath L.H. A Review on Automatic Fault Detection and Diagnosis in a Single Point Cutting Tool Using Wavelet Analysis. *International Journal of Advances in Scientific Research and Engineering*. 2017. No. 3(1). Pp. 230–234.

12. Simoens P., Dragone M., Saffiotti A. The Internet of Robotic Things: A review of concept, added value and applications. *International Journal of Advanced Robotic Systems I–II.* 2018. Pp. 1–9.

13. Goreva T.I., Pornyagin N.N., Pyukke G.A. Nejrosetevye modeli diagnostiki tekhnicheskih system [Neural network model for diagnosis of technical systems]. Vestnik KRAUNC. Fiz-mat. nauki [Vestnik kraunc. Physical and mathematical sciences]. 2017. No. 1 (4). Pp. 31–43. (In Rus)

14. Vinogradenko A.M., Zayac S.V., Kuznecov S.V. Perspektivy razvitiya polevyh i stacionarnyh sredstv tekhnicheskogo obespecheniya [Prospects for the development of field and stationary technical support facilities]. *Materialy III VNPK "Sovremennye problemy sozdaniya i ekspluatacii VVST"* [Materials of the III VNPK "Modern problems of creation and operation of vvst»]. St. Petersburg, 2019. Pp. 15–18. (In Rus)

15. Zołtowski M., Martinod R. Technical Condition Assessment of Masonry Structural Components using Frequency Response Function (FRF). *Journal of the International Masonry Society Masonry International*. 2016. Vol 29(1). Pp. 23–27.

16. Hahanov V.I., Shcherba O.V. Primenenie iskusstvennyh nejronnyh setej dlya diagnostirovaniya cifrovyh setej [Application of artificial neural networks for diagnosing digital networks]. *Radioelektronnye i komp'yuternye sistemy* [Radioelectronic and computer systems]. 2017. No. 5 (46). Pp. 15–20. (In Rus)

17. Antonyuk E.M., Lomonosova Yu.S. Sistemy avtomaticheskogo kontrolya so szhatiem dannyh [Automatic control systems with data compression]. *Izvestiya SPbGETU (LETI)* [**I**zvestiya SPbGETU (LETI)]. 2017. No. 7. Pp. 62–68. (In Rus)

18. Klimov V.V., Krapivin V.F., Mkrtchyan F.A., Nichipor A.E. Metody klassifikacii i kachestvennoj interpretacii dannyh distancionnogo monitoringa okruzhayushchej sredy [Methods of classification and qualitative interpretation of remote environmental Monitoring Data]. *Ekologicheskie sistemy i pribory* [Environmental systems and devices]. 2019. No. 3. Pp. 7–12. (In Rus)

19. Volobuev M.F., Ufaev V.A. Obnaruzhenie postepennyh otkazov v rezervirovannoj izmeritel'noj sisteme v zavisimosti ot polnoty veroyatnostnogo opisaniya vyhodnyh signalov [Detection of gradual failures in a redundant measurement system depending on the completeness of the probabilistic description of output signals]. *Informacionno-izmeritel'nye i upravlyayushchie sistemy* [Information-measuring and control systems]. 2017. Vol. 15. No. 10. Pp. 28–35. (In Rus)

20. Volobuev M.F., Mal'cev A.M., Mihajlenko S.B., Ufaev V.A. Sposob obnaruzheniya otkazov pri ekonomichnom rezervirovanii bortovogo oborudovaniya bespilotnogo letatel'nogo apparata [Method for detecting failures in the economical reservation of onboard equipment of an unmanned aerial vehicle]. *Zhurnal Sibirskogo federal'nogo universiteta. Tekhnika i tekhnologii* [Journal of the Siberian Federal University. Equipment and technologies]. 2016. No. 9 (7). Pp. 1060–1067. (In Rus)

INFORMATION ABOUT AUTHORS:

Abramkin R.V., postgraduate student of the S. M. Budyonny Military Academy of Communications;

Pedan A.V., PhD, Senior Lecturer of the S. M. Budyonny Military Academy of Communications;

Vinogradenko A.M., PhD, Docent, Doctoral Candidate Military academy of communications named after Marshal of the Soviet Union S.M. Budyonny.

For citation: Abramkin R.V., Pedan A.V., Vinogradenko A.M. Methodology for monitoring and predicting the technical condition of the secondary power supply system of field communication objects based on a neural network campaign. *H&ES Research*. 2021. Vol. 13. No. 3. Pp. 4–18. Doi: 10.36724/2409-5419-2021-13-3-4-18 (In Rus)

ЗАО "НПЦ ИРС" НИУ "МИЭТ" ООО "ИНТЕХ"

МОСКВА 20.10.2021

НАУКА И АСУ 2021

ВСЕРОССИЙСКАЯ МЕЖВЕДОМСТВЕННАЯ НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ

по теоретическим и прикладным проблемам развития и совершенствования АСУ и связи специального назначения

http://intech-spb.com/conferences/
konferencia_asu_vka@mail.ru

Тематика конференции включает работу следующих секций:

01

Состояние и перспективы развития современных автоматизированных систем управления специального назначения

02

Математическое, программное и информационно-лингвистическое обеспечение автоматизированных систем управления

03

Безопасность в автоматизированных системах управления специального назначения

04

Применение современных инфокоммуникационных технологий и средств при разработке, техническом обеспечении и эксплуатации автоматизированных систем управления специального назначения

05

Состояние и перспективы развития систем, комплексов и средств адиосвязи специального назначения

06

Проблемы развития автоматизированных систем управления технологическим процессом

КРУГЛЫЙ СТОЛ

Цифровая психология: Использование математических методов при прогнозировании развития личности человека

НИУ МИЭТ
Москва, Зеленоград

20 октября

По итогам конференции отобранные оргкомитетом доклады в виде статей будут опубликованы в журналах из Перечня ВАК, РИНЦ

T-comm • Информация и космос • H&ES Research • I-methods • Техника средств связи

Участие в конференции и публикация материалов в сборнике тезисов БЕСПЛАТНО.

Doi: 10.36724/2409-5419-2021-13-3-20-27

ОПРЕДЕЛЕНИЕ МНОГОКРИТЕРИАЛЬНОГО ПОКАЗАТЕЛЯ КАЧЕСТВА ГРАФИЧЕСКОГО ИНТЕРФЕЙСА ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА СВЯЗИ

ФЕДОРОВА
Светлана Викторовна

АННОТАЦИЯ

Введение: повышение степени автоматизации разрабатываемых средств и комплексов связи влечет за собой увеличении сложности программных продуктов их управления. Ввиду ограниченных возможностей человека, встает вопрос об эргономичности человеко-машинных интерфейсов, а именно программного пользовательского интерфейса, позволяющем увеличить эффективность всей человеко-машинной системы. **Цель исследования:** целью исследования является определение структуры и состава программного пользовательского интерфейса, его параметров, оказывающих влияние на надежность деятельности оператора при управлении программно-аппаратным комплексом связи. **Методы:** поскольку современные методы оценки программных интерфейсов не позволяют произвести всестороннюю количественную оценку его параметров, решение задачи предлагается осуществить с использованием методов теории систем выявляя количественные, достоветные и объективные сведения об исследуемом программном пользовательском интерфейсе. Предлагаемое математическое описание программного пользовательского интерфейса необходимо для определения показателя качества интерфейса, отражающего степень его эргономичности. **Результаты:** использование предлагаемого математического описания программного пользовательского интерфейса основанного на определении параметров элементов, входящих в его состав, и дальнейшее определение многокритериального показателя его качества и эргономичности позволит оценить влияние значений параметров элементов интерфейса на показатель его качества, а при проектировании сложных интерфейсов изменение этих параметров позволит проанализировать и выявить такие параметры элементов пользовательского интерфейса, при которых показатель его качества имеет наилучшие значения. **Практическая значимость:** представленные результаты предлагается использовать при проведении оценки функциональной надежности перспективных разрабатываемых программно-аппаратных комплексов связи и моделировании процесса взаимодействии оператора с этим комплексом посредством программного пользовательского интерфейса. **Вывод:** оценка функциональной надежности программно-аппаратного комплекса связи основанная на результатах взаимодействия оператора с программным пользовательским интерфейсом комплекса связи, многокритериальный показатель качества которого отражает степень его эргономичности, позволит на стади проектирования перспективных программно-аппаратных комплексов связи оценить влияние параметров элементов интерфейса на безошибочность действий оператора.

КЛЮЧЕВЫЕ СЛОВА: пользовательский интерфейс; графический интерфейс; качество интерфейса; показатель качества;эргономическая оценка интерфейса.

Сведения об авторе:
адъюнкт Военной академии связи им. С.М. Буденного, г. Санкт-Петербург, Россия, svetafedorov@mail.ru

Для цитирования: *Федорова С.В.* Определение многокритериального показателя качества графического интерфейса программно-аппаратного комплекса связи // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13. № 3. С. 20–27. Doi: 10.36724/2409-5419-2021-13-3-20-27

Введение

Развитие и разработка перспективных комплексов средств связи и автоматизации управления неотъемлемо связаны с повышением степени автоматизации рабочего места оператора. Управление техникой за счет использования программно-аппаратных средств приводит к повышению производительности, сокращению времени выполнения процесса, увеличению точности и стабильности выполняемых операций. Взаимодействие оператора с программным обеспечением комплекса — основная составляющая его деятельности. Это взаимодействие осуществляется через пользовательский интерфейс, включающий аппаратную и программную составляющую. Аппаратный пользовательский интерфейс представляет собой устройства ввода, вывода и отображения информации, используемые при осуществлении диалога с программой управления программно-аппаратным комплексом. Программный пользовательский интерфейс непосредственно обеспечивает диалог оператора с программой и визуализацию элементов управления комплексом на экране. Наиболее широкое применение получил графический интерфейс типа «Window (окно), Image (образ), Menu (меню), Pointer (указатель)» (WIMP) [1,2].

К настоящему времени проведено достаточное количество исследований [3–5] доказывающих влияние пользовательского интерфейса на результат трудовой деятельности операторов. Так «плохо» спроектированный пользовательский интерфейс может стать источником стресса и психологического дискомфорта оператора, которые приведут к уменьшению производительности оператора и возрастанию количества ошибок в его работе.

Анализ существующих методик оценки эргономичности графического интерфейса

Проектирование и разработка графического пользовательского интерфейса (далее интерфейса), как правило, возложены на специалиста осуществляющего проектирование и разработку всего программного обеспечения образца техники [6–8]. Такой специалист обычно не обладает знаниями в области эргономики программного обеспечения и «пишет» интерфейс лишь с учетом выполняемых техникой функций, заданных в тактико-техническом задании заказчиком и собственными субъективными представлениями о понятности и удобстве интерфейса. А так как около 80% информации человек получает через органы зрения, вопрос построения интерфейса крайне важен [9]. Это построение не может и не должно быть исключительно интуитивным, а значит, необходимы формальные методики, модели и алгоритмы для выполнения этих задач.

В настоящее время существует серии стандартов ГОСТ Р ИСО 9241, ГОСТ Р ИСО 14915, ГОСТ РВ 0029 и др., касающиеся эргономики программного обеспечения и устанавливающие требования, правила и рекомендации проектирования пользовательских интерфейсов — как общецелевых, так и специализированных. Оценка уровня эргономичности интерфейса проводится с помощью контрольного списка применимости и соответствия требованиям, критерии которых двоичны (да/нет). Для допустимого и высокого уровня эргономичности отношение количества выполненных требований к общему количеству требований, применимых к оцениваемому интерфейсу — показатель степени выполнения эргономических требований $K_{инт}$ должен быть не менее 0,80. Существующая система стандартов позволяет определить соответствие требованиям, но не предоставляет точного оценочного критерия и методических средств анализа разработанного интерфейса, не позволяет провести количественную оценку его параметров качества, в том числе и эргономических.

На сегодняшний день существует достаточно много методик оценки эргономичности интерфейса [10], но они используются разрозненно, в зависимости от принятых у разработчиков способов его разработки и методов оценки. К таким методам относятся:

– оценка, основанная на сравнении и соответствии среде;

– экспертная оценка;

– анкетирование пользователей;

– количественная оценка, базирующаяся на экспериментальных данных;

– формальные методы оценки (информационный поиск, информационная производительность (закон Хика), модель GOMS, оценка сложности системы Тима Комбера и Джона Мелтби, XAOS — модель (визуальная сложность интерфейса), LOC–CC модель автоматического тестирования).

Каждый из этих методов обладает рядом недостатков и не позволяет с достаточной полнотой дать оценку по всем эргономическим параметрам интерфейса с учетом высоких темпов развития в области информационных технологий. Например, методы с привлечением экспертов имеют большую продолжительность и не имеют доказательств правильности, методы с привлечением реальных пользователей не всегда реализуемы, а потенциальный недостаток существующих методов количественных и формальных оценок — неэтичность оценки работы человека по одному параметру, по которому в дальнейшем судить о производительности и удобстве интерфейса в целом.

– Анализ недостатков существующих методик оценки эргономичности интерфейса указывает о необходимости решения следующих проблем:

– необходимо формальное математическое описание интерфейса — описание его структуры, введение параметров и их количественная оценка;

– необходимы многокритериальная методика и алгоритм оценки интерфейса;

– необходимо определение критериев и условий оптимальности интерфейса, соответствующие требованиям эргономичности.

Математическое описание графического интерфейса

Графические пользовательские интерфейсы большинства прикладных программ используемых в современных программно-аппаратных комплексах связи и автоматизированных системах управления построены на основе стандартных элементов управления, предоставляемых графической оболочкой операционной системы. В интерфейсах такого типа преобладают статические элементы, предназначенные для ввода и вывода информации. В связи с этим дальнейшая работа будет ориентирована на описание и оценку графического пользовательского интерфейса такого типа [1].

Математическая модель интерфейса F представляет собой упорядоченный набор величин: S — структурного описания интерфейса, B — описания интерфейса как целостного графического образа — битовой карты, M — множество характеристик дискретной координатной плоскости интерфейса

$$F = \langle S, B, M \rangle.$$

Структурное описание интерфейса представляет собой совокупность описаний множества элементов, из которых состоит интерфейс и взаимосвязей между ними. Поскольку в графическом пользовательском интерфейсе WIMP-типа любой элемент может содержать в себе другие элементы, т.е. как бы быть контейнером для других, имеет место отношение подчиненности между элементами, формирующее их древовидную структуру. Начальная экранная форма интерфейса является при этом главным контейнером, внутри которого размещены все его элементы. Расположение элемента внутри контейнера определяется его координатами в соответствии с характеристиками координатной плоскости M. А именно, элемент m-уровня ограничивает элементы расположенные внутри него, т.е. элементы подуровня, входящие в его состав, не могут выходить за границы элемента, в котором они расположены. Границы элемента m-уровня определяются характеристиками этого элемента в координатной плоскости. Они размещают (ограничивают, выравнивают) элементы координатами, началом которых является верхний левый угол, а координатные оси направлены вправо и вниз.

Таким образом структурное описание интерфейса имеет вид:

$$S = \langle S^n \rangle,$$

где S^n — элемент интерфейса, индекс которого определяет его положение в структуре и взаимосвязь между элементами.

При этом структурное описание самого элемента имеет следующий вид:

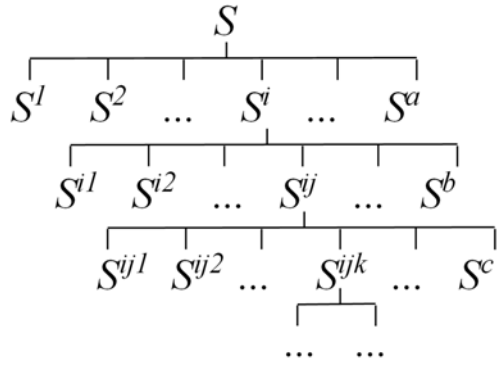
$$S^n = \langle P^n, S^{nm}, \alpha^n \rangle,$$

где P^n — множество параметров элемента с индексом n, S^{nm} — множество элементов, входящих в его состав, α^n — линейный порядок во множестве S^{nm}, определяющий последовательность элементов в S^n.

Поскольку в графических пользовательских интерфейсах WIMP-типа пользователь может интерактивно взаимодействовать только с одним элементом интерфейса линейный порядок α^n определяет цепочку перемещения между елементами.

Структура элементов интерфейса будет иметь вид, представленный на рисунке.

Множество характеристик метрики дискретной координатной плоскости интерфейса представляет собой выражение вида: $M = \langle \Delta_x, \Delta_y, N_x, N_y \rangle$, где Δ_x — шаг по



Структурная схема множества элементов ГПИ

оси абсцисс (мм), Δ_y — шаг по оси ординат (мм), N_x — число узлов координатной сетки по оси абсцисс, N_y –число узлов координатной сетки по оси ординат. Все координаты $\langle x, y \rangle$ в плоскости экранной формы интерфейса определены таким образом, что их значения кратны Δ_x и Δ_y соответственно.

Битовая карта графического интерфейса — матрица чисел $B = [b_{ij}], i = 1...N_x, j = 1...N_y$ — состоит из элементарных элементов изображения (пикселей) и представляет собой множество прямоугольных областей b_{ij}, имеющих геометрические размеры $\Delta_x \times \Delta_y$, каждый из которых окрашен одним цветом c_{ij}. Следовательно, каждая прямоугольная область представляет собой $b_{ij} = \langle x_{ij}, y_{ij}, c_{ij} \rangle$, где $x_{ij} = i \cdot \Delta_x, y_{ij} = j \cdot \Delta_x$. Цвет c_{ij} задается параметрами аддитивной цветовой модели RGB, поскольку в настоящее время большинство устройств отображения информации построены по принципу «излучения» света [11–13].

Математическое описание элемента графического интерфейса

Для структурного описания элемента интерфейса S^n необходимо определить его основные параметры, и составить по ним математическую модель элемента интерфейса, которая будет универсальной по отношению к основным элементам интерфейса WIMP-типа[1,2,3].

Основные элементы интерфейса данного типа можно разделить на две группы. К первой группе относятся элементы, предназначенные для ввода/вывода информации и команд от пользователя (меню, полоса прокрутки, блок списка, редакторы, кнопки и т.д.), ко второй — только для вывода информации и оформления других элементов (статический текст, блок группировки, курсор графического манипулятора, индикатор процесса и т.д.).

У каждого элемента можно выделить следующие основные параметры:

– информационные параметры элемента I, представляющие собой множество надписей T, множество изображений P, уровни информационной нагруженности I_{in} и I_{out}

$$I = \langle T, P, I_{in}, I_{out} \rangle;$$

– визуальные параметры элемента D (параметры оформления): используемый шрифт fnt, кегель k, начертание s, цвет текста (переднего плана) frt и фона b, используемые изменения m текста (например, подчеркивание), используемые эффекты e (например, мерцание текста)

$$D = \langle fnt, k, s, frt, b, m, e \rangle;$$

– геометрическое расположение элемента на экранной форме интерфейса, заданная его контуром L — замкнутая ломаная линия, являющаяся упорядоченной последовательностью точек с координатами x и y , ограниченная характеристиками метрики M

$$L = \langle (x_1, y_1), ..., (x_i, y_i) \rangle, i = 1, 2, 3, ...$$

Таким образом, параметры элемента интерфейса можно формально описать следующим набором:

$$P^n = \langle I, D, L \rangle = \left\langle \begin{array}{l} I = \langle T, P, I_{in}, I_{out} \rangle \\ D = \langle fnt, k, s, frt, b, m, e \rangle \\ L = \langle (x_1, y_1), ..., (x_i, y_i) \rangle \end{array} \right\rangle.$$

Тогда формальное описание элемента интерфейса будет иметь вид:

$$S^n = \langle P^n, S^{nm}, \alpha^n \rangle = \left\langle \begin{array}{l} I = \langle T, P, I_{in}, I_{out} \rangle \\ D = \langle fnt, k, s, frt, b, m, e \rangle \\ L = \langle (x_1, y_1), ..., (x_i, y_i) \rangle \\ S^{nm} = \langle P^{nm}, S^{nmw}, \alpha^{nm} \rangle \\ \alpha^n \end{array} \right\rangle = ... \quad (1)$$

Математическая модель самого графического пользовательского интерфейса представляет собой следующее выражение:

$$F = \langle S, B, M \rangle = \left\langle \begin{array}{l} S^n = \langle P^n, S^{nm}, \alpha^n \rangle \\ M = \langle \Delta_x, \Delta_y, N_x, N_y \rangle \\ B = \left[b_{ij} \right] \end{array} \right\rangle =$$

$$= \left\langle \begin{array}{l} M = \langle \Delta_x, \Delta_y, N_x, N_y \rangle \\ B = \left[b_{ij} \right] \\ S^n = \left\langle \begin{array}{l} I^n = \langle T, P, I_{in}, I_{out} \rangle \\ D^n = \langle fnt, k, s, frt, b, m, e \rangle \\ L^n = \langle (x_1, y_1), ..., (x_i, y_i) \rangle \\ S^{nm} = \langle P^{nm}, S^{nmw}, \alpha^{nm} \rangle \\ \alpha^n \end{array} \right\rangle \end{array} \right\rangle = ... \quad (2)$$

Многоточие в формулах 1 и 2 означает, что данное математическое описание не конечно, но имеет ограничения в соответствии с количеством уровней элементов в структуре интерфейса.

Операторы описания

Используя полученные математические описания интерфейса и его элементов (формулы 1 и 2) введем операторы, необходимые для оценки качества элементов и интерфейса[4] [14].

Множество всех элементов, входящих в состав интерфейса

$$\Theta_S(F) = \left\{ S, S^1, ..., S^{1...z}, S^2, ..., S^{2...q}, ..., S^n, ..., S^{n...m} \right\}.$$

[1]Вадзинский Р. Н. Справочник по вероятностным распределениям. СПб.: Наука, 2016. 295 с.

[2]Венцель Е.С. Теория вероятностей. 10-е изд., стер. М.: Академия, 2017. 576 с.

[3]Виленкин Н. Я., Куницкая Е. С., Мордкович А. Г. Математический анализ. Интегральное исчисление. М.: Просвещение, 2016. 176 с.

[4]Мальцев А.И. Алгебраические системы. М.: Наука, 2017. 392 с.

Общее количество элементов в структуре интерфейса — мощность множества элементов

$$\Theta_N(F) = \left|\Theta_S(F)\right|.$$

Битовая карта (графический образ) элемента интерфейса S^n

$$\Theta_B\left(S^n\right) = \left\{\left(b_{ij} = \left\langle x_{ij}, y_{ij}, c_{ij}\right\rangle \in F \to B\right) : \left(x_{ij}, y_{ij}\right) \in L\right\}.$$

Битовая карта (графический образ) покрываемая кортуром L

$$\Theta_B(F, L) = \left\{\left(b_{ij} = \left\langle x_{ij}, y_{ij}, c_{ij}\right\rangle \in F \to B\right) : \left(x_{ij}, y_{ij}\right) \in L\right\}.$$

Оператор построения цвета модели RGB по величинам трех составляющих r, g, b

$$\Theta_{RGB}(r, g, b).$$

При этом величина красной цветовой составляющей цвета с равна $\Theta^R(c) = R(c) \in [0,1]$, зеленой — $\Theta^G(c) = G(c) \in [0,1]$, синей — $\Theta^B(c) = B(c) \in [0,1]$.

Евклидова метрика «цветового расстояния», задающая расстояние между двумя цветами c_i и c_j определяется следующим выражением:

$$d_c^2(c_i, c_j) = \left(\Theta^R(c_i) - \Theta^R(c_j)\right)^2 + \left(\Theta^G(c_i) - \Theta^G(c_j)\right)^2 + \left(\Theta^B(c_i) - \Theta^B(c_j)\right)^2.$$

Координаты элемента интерфейса имеют значение координаты точки верхнего левого угла элемента

$$\Theta_{xy}\left(S^n\right) = \left\langle x^n, y^n\right\rangle = \left\langle \min\left(x_i\right), \min\left(y_i\right)\right\rangle : \left\langle x_i, y_i\right\rangle \in L \subset Q.$$

Качество графического интерфейса, элемента и их показатели

Качество графического пользовательского интерфейса, как и большинства других систем, напрямую зависит от качества входящих в его состав элементов [1, 14, 16]. Качество элемента Q_{S^n}, в соответствии с предложенными математическим описанием и основными параметрами, будем определять по следующим его составляющим показателям:

– визуальная эффективность *Vis* (visual) — степень соответствия внешнего вида элемента выполнению поставленных перед ним задач;

– информационная эффективность *Inf* (information) — соответствие информационных параметров элемента его назначению и выполняемых им функций;

– геометрическая эффективность *Arr* (arrange) — правильность расположения элемента в структуре интерфейса;

– уместность *Com* (compatibility) — необходимость и совместимость элемента в контексте реализации ГПИ в целом.

$$Q_{S^n} = Vis + Inf + Arr + Com. \quad (3)$$

Необходимо также отметить, что графический пользовательский интерфейс техники в целом состоит из элементов различного назначения: элементы управления техникой, сервисные элементы, элементы оформления, вспомогательные элементы. Далее будут рассмотрены только элементы управления техникой, так как для осуществлении трудовой деятельности оператору необходимо взаимодействие с этими элементами.

Как уже отмечалось выше, основными элементами графического интерфейса являются: статический текст или изображение *St* (наприме, индикатор процесса), полоса прокрутки *Scr*, блок списка (список) *Bx*, редакторы (текстовые и числовые) *Ed*, кнопки *Bt*.

Тогда качество группы однотипных элементов представляет собой среднее значение качества елементов, входящих в группу. Например, для группы элементов статического текста качество группы элементов будет иметь вид:

$$Q_{St} = \frac{\sum_{i=1}^{n} k_i \cdot Q_{St_i}}{n}, \quad (4)$$

где n — количество елементов в группе, k_i — весовой коэффициент значимости элемента в интерфейсе в целом, определяется для каждого элемента интерфейса, основываясь на алгоритме анализа иерархий, при этом сумма коэффициентов в группе равна единице $\sum_{i=1}^{n} k_i = 1.$

Суммируя средние показатели качества групп элементов, можно определить общий показатель качества интерфейса:

$$Q = Q_{St} + Q_{Scr} + Q_{Bx} + Q_{Ed} + Q_{Bt}. \quad (5)$$

Используя выражения 3–5 можно оценить качество интерфейса по одному из показателей качества элементов, например определение визуальной эффективности интерфейса будет иметь вид:

$$Q_{Vis} = Vis_{St} + Vis_{Scr} + Vis_{Bx} + Vis_{Ed} + Vis_{Bt}. \quad (6)$$

При это визуальная эффективность группы элементов статического текста (изображения) определяется по формуле:

$$Vis_{St} = \frac{\sum_{i=1}^{n} k_i \cdot Vis_{St_i}}{n}.$$

Для остальных групп элемента визуальная эффективность определяется подобным способом.

Проанализируя формулы 3,5,6 справедливо следующее выражение, определяющее качество интерфейса:

$$Q = Q_{Vis} + Q_{Inf} + Q_{Arr} + Q_{Com}.$$

Таким образом, определив параметры элементов интерфейса можно формально описать качество не только элемента, но и провести ее улучшение для повышения показателя качества интерфейса. А имея функцию качества, можно провести ее улучшение для повышения показателя качества интерфейса. Не смотря на концептуальную простоту, предложенный подход дает общий способ оценки качества интерфейса.

Заключение

Надежность сиситемы оператор — программно-аппаратный комплекс совокупная характеристика техники и обслуживающих ее людей. Безошибочность и надежность деятельности оператора зависит от эргономических показателей техники, к которым относятся как эргономические показатели организации рабочего места, так и эргономические показатели формы и вида предъявления потока рабочей информации, а для оператора программно-аппаратного комплекса это программный пользовательский интерфейс. В связи с развитием современных технологий и повышением степени автоматизации рабочих мест оператора, оценка эргономичности пользовательского интерфейса становится особенно актуальной. Полученные формальное математическое описание интерфейса и элементов, входящих в его состав, выявленные параметры используемых в интерфейсе элементов и вычисленный с их помощью многокритериальный показатель качества интерфейса, исключают ряд недостатков существующих методик оценки эргономичности интерфейса. Основанная на полученных результатах методика оценки эргономичности интерфейса позволит получить количественные, достоверные и объективные сведения о графическом пользовательском интерфейсе, которые сложно получить без проведения вычислений (например, методом экспертных оценок).

Литература

1. *Семёнов С.С., Фёдоров В.Г., Фёдорова С.В.* Классификация пользовательских интерфейсов программно-аппаратных комплексов связи и автоматизированных систем управления военного назначения // Сборник трудов III Межвузовской научно-практической конференции «Проблемы технического обеспечения войск в современных условиях». СПб.: ВАС, 2018. Т. 1. С. 360–366.

2. Федоров В.Г., Федорова С.В., Спицын О.Л. Способ выделения структурно-топологических неоднородностей заданного фрагмента сети связи. // I-methods. 2019. Т. 11. № 2. С. 1–13

3. *Shneiderman B., Plaisant C., Cohen M., Jacobs S. Elmqvist N., Diakopoulos N.* Designing the User Interface: Strategies for Effective Human — Computer Interaction. 6th Edition. Pearson. 2017. 624 p.

4. *Бурков Е.А., Падерно П.И., Сопина О.П.* Анализ и комплексирование методов оценки алгоритмов деятельности // Труды Третьей Международной научно-практической конференции «Человеческий фактор в сложных технических системах и средах» (Эрго-2018). (Санкт-Петербург, Россия, 4–7 июля 2018) / Под ред. А. Н. Анохина, А. А. Обознова, П. И. Падерно, С. Ф. Сергеева. СПб.: СПбГЭТУ «ЛЭТИ», Межрегиональная эргономическая ассоциация, 2018. С. 275–281.

5. *Казаков А.В., Кипер А.В.* Эксплуатационно-технические характеристики интерфейсов автоматизированных комплексов связи в математической модели оценки надежности деятельности человека-оператора // Сборник трудов II Межвузовской научно-практической конференции «Проблемы технического обеспечения войск в современных условиях». СПб.: ВАС, 2017. Т. 1. С. 117–121.

6. *Анохин А.Н., Малишевский В.*С. Методы предпроектного анализа при создании операторского интерфейса. // Труды Второй Международной научно-практической конференции «Человеческий фактор в сложных технических системах и средах» (Эрго-2016). СПб.: Межрегиональная эргономическая ассоциация, ФГАОУ ДПО «ПЭИПК», Северная звезда, 2016. С. 357–363.

7. *Семёнов С.С., Фёдорова С.В. Мешков С.А.* Решение задачи оценки надежности функционирования системы «человек — машина» с использованием показателя эффективности взаимодействия оператора и программно — аппаратного комплекса связи военного назначения // Материалы межведомственной научно-теоретической конференции «Актуальные вопросы развития технического обеспечения в современных условиях». СПб.: ВА МТО, 2018. Ч. 8. С. 162–169.

8. *Федоров В.Г., Стародубцев Ю.И., Бегаев А.Н.* Методика оценки управляемости фрагмента сети связи общего пользования с учетом влияния множественности центров управления и деструктивных программных воздействий // Вопросы кибербезопасности. 2017. № 4(22). С. 32–39.

9. *Коморников П.М., Морозов Р.В., Фатьянова Е.В.* О подходах в оценке надежности системы «оператор — аппаратно-программные средства связи» // Сборник трудов III Межвузовской научно-практической конференции «Проблемы технического обеспечения войск в современных условиях». СПб.: ВАС, 2018. Т. 1. С. 303–307

10. *Евсевичев Д.А., Самохвалов М.К.* Автоматизация расчета эргономических параметров средств отображения информации на рабочем месте авиадиспетчера // Информационные системы. 2017. № 3 (49). С. 70–78.

11. *Aalipour M., Ayele Y.Z., Barabadi A.* Human reliability assessment (HRA) in maintenance of production process: a case study // International Journal of System Assurance Engineering and Management. 2016. No. 7. Pp. 229–238.

12. *Чернышева О.Н.* Проблемы нормирования параметров предметной среды и ее эргономическая оценка и проектирование // Труды Второй международной научно-практической конференции «Человеческий фактор в сложных технических системах и средах» (Эрго 2016). (Санкт-Петербург, Россия, 6–9 июля 2016) / Под ред. А. Н. Анохина, П. И. Падерно, С. Ф. Сергеева. — СПб.: Межрегиональная

эргономическая ассоциация, ФГАОУ ДПО «ПЭИПК», Северная звезда, 2016. С. 83–86.

13. *Стародубцев Ю. И., Федоров В. Г.* Способ обнаружения источника сетевых атак на автоматизированные системы // Проблемы экономики и управления в торговле и промышленности. 2016. № 1 (13). С. 87–92.

14. *Алюшин М. В., Талалаев А. А.* Обеспечение надежности профессиональной деятельности эксплуатационного и диспетчерского персонала электроэнергетики // Труды Третьей Международной научно-практической конференции «Человеческий фактор в сложных технических системах и средах» (Эрго-2018). (Санкт-Петербург, Россия, 4–7 июля 2018) / Под ред. А. Н. Анохина, А. А. Обознова, П. И. Падерно, С. Ф. Сергеева.— СПб.: СПбГЭТУ «ЛЭТИ», Межрегиональная эргономическая ассоциация, 2018. С. 306–314.

15. *Богомолов А. В., Зинкин В. Н., Алёхин М. Д., Свиридюк Г. А., Келлер А. В.* Информационно-логическое моделирование сбора и обработки информации при оценивании функциональной надежности оператора авиационных эргатических систем управления // Труды Третьей Международной научно-практической конференции «Человеческий фактор в сложных технических системах и средах» (Эрго-2018). (Санкт-Петербург, Россия, 4–7 июля 2018) / Под ред. А. Н. Анохина, А. А. Обознова, П. И. Падерно, С. Ф. Сергеева. СПб.: СПбГЭТУ «ЛЭТИ», Межрегиональная эргономическая ассоциация, 2018. С. 315–323.

16. *Стародубцев Ю. И., Чукариков А. Г., Корсунский А. С., Федоров В. Г.* Способ защиты инфотелекоммуникационных сетей критически важных объектов от сетевых компьютерных атак // Автоматизация процессов управления. 2018. № 1 (51). С. 14–19.

DETECTION OF A MULTI-CRITERIA INDICATOR OF THE QUALITY OF THE GRAPHICAL INTERFACE OF THE SOFTWARE AND HARDWARE COMMUNICATION COMPLEX

SVETLANA V. FEDOROVA

Saint Petersburg, Russia, svetafedorov@mail.ru

KEYWORDS: user interface; graphical interface; interface quality; quality indicator;ergonomic evaluation of the interface.

ABSTRACT

Introduction: increasing the degree of automation of the developed means and communication complexes entails an increase in the complexity of software products for their management. Due to the limited human capabilities, the question arises about the ergonomics of human-machine interfaces, namely, the software user interface, which allows to increase the efficiency of the entire human-machine system. **The purpose** of the study is to determine the structure and composition of the software user interface, its parameters that affect the reliability of the operator's activities when managing the software and hardware complex of communication. **Methods:** since modern methods of evaluating software interfaces do not allow for a comprehensive quantitative assessment of its parameters, the solution of the problem is proposed to be carried out using the methods of system theory, revealing quantitative, reliable and objective information about the software user interface under study. The proposed mathematical description of the software user interface is necessary to determine the quality indicator of the interface, reflecting the degree of its ergonomics. **Results:** the use of the proposed mathematical description of the software user interface based on the definition of the parameters of the elements that make up it, and the further definition of the multi-criteria indicator of its quality and ergonomics will allow us to assess the impact of the values of the parameters of the interface elements on the indicator of its quality, and when designing complex interfaces, changing these parameters will allow us to analyze and identify such parameters of the user interface elements, in which the indicator of its quality has the best values. **Practical significance:** the presented results are proposed to be used in assessing the functional reliability of promising developed software and hardware communication systems and modeling the process of operator interaction with this complex through a software user interface. **Conclusion:** the evaluation of the functional reliability of the software and hardware communication complex based on the results of the operator's interaction with the software user interface of the communication complex, the multi-criteria quality indicator of which reflects the degree of its ergonomics, will allow at the design stage of promising software and hardware communication complexes to assess the influence of the parameters of the interface elements on the error-free actions of the operator.

REFERENCES

1. Semenov S.S., Fedorov V.G., Fedorova S.V. Klassifikacija pol'zovatel'skih interfejsov programmno-apparatnyh kompleksov svjazi i avtomatizirovannyh sistem upravlenija voennogo naznachenija [Classification of user interfaces of software and hardware communication systems and automated control systems for military purposes]. *Sbornik trudov III Mezhvuzovskoj nauchno-prakticheskoj konferencii "Problemy tehnicheskogo obespechenija vojsk v sovremennyh uslovijah"* [Proc. of the III Interuniversity scientific and practical conference "Problems of technical support of troops in modern conditions"]. St. Petersburg: VAS, 2018. Vol. 1. Pp. 360–366. (In Rus)

2. Fedorov V.G., Fedorova S.V., Spitsyn O.L. A method for identifying structural and topological inhomogeneities of a given fragment of a communication network. *I-methods*. 2019. Vol. 11. No. 2. Pp. 1–13. (In Rus)

3. Shneiderman B., Plaisant C., Cohen M., Jacobs S. *Elmqvist N., Diakopou-*

los N. Designing the User Interface: Strategies for Effective Human – Computer Interaction. 6th Edition. Pearson, 2017. 624 p.
4. Burkov E.A., Paderno P.I., Sopina O.P. Analiz i kompleksirovanie metodov ocenki algoritmov dejatel'nosti [Analysis and integration of methods for evaluating algorithms of activity]. *Trudy Tret'ej Mezhdunarodnoj nauchno-prakticheskoj konferencii "Chelovecheskij faktor v slozhnyh tehnicheskih sistemah i sredah".* [Proc. of the Third International Scientific and Practical Conference "The human factor in complex technical systems and environments" (Ergo-2018)]. (St. Petersburg, Russia, July 4–7, 2018) Ed. by A.N. Anokhin, A.A. Oboznov, P.I. Paderno, S.F. Sergeev. St. Petersburg: SPbGETU "LETI", Interregional Ergonomic Association, 2018. Pp. 275–281. (In Rus)
5. Kazakov A.V. Kiper A.V. Jekspluatacionno-tehnicheskie harakteristiki interfejsov avtomatizirovannyh kompleksov svjazi v matematicheskoj modeli ocenki nadezhnosti dejatel'nosti cheloveka-operatora [Operational and technical characteristics of interfaces of automated communication complexes in a mathematical model for evaluating the reliability of human operator activity]. *Sbornik trudov II Mezhvuzovskoj nauchno-prakticheskoj konferencii "Problemy tehnicheskogo obespechenija vojsk v sovremennyh uslovijah"* [Proc. of the II Interuniversity scientific and practical conference "Problems of technical support of troops in modern conditions"]. St. Petersburg: VAS, 2017. Vol. 1. Pp. 117–121. (In Rus)
6. Anokhin A.N., Malishevsky V.S. Metody predproektnogo analiza pri sozdanii operatorskogo interfejsa [Methods of pre-project analysis when creating an operator interface]. *Trudy Vtoroj Mezhdunarodnoj nauchno-prakticheskoj konferencii "Chelovecheskij faktor v slozhnyh tehnicheskih sistemah i sredah"*. [Proc. of the Second International scientific and practical conference "The Human factor in complex technical systems and environments" (Ergo-2016)]. Saint Petersburg: interregional ergonomic Association, North star, 2016. Pp. 357–363. (In Rus)
7. Semenov S.S., Fedorova S.V. Meshkov S.A. Reshenie zadachi ocenki nadezhnosti funkcionirovanija sistemy "chelovek – mashina" s ispol'zovaniem pokazatelja jeffektivnosti vzaimodejstvija operatora i programmno – apparatnogo kompleksa svjazi voennogo naznachenija [Solving the problem of evaluating the reliability of the "man – machine" system using the efficiency indicator of interaction between the operator and the software and hardware complex of military communications]. *Materialy mezhvedomstvennoj nauchno-teoreticheskoj konferencii "Aktual'nye voprosy razvitija tehnicheskogo obespechenija v sovremennyh uslovijah"* [Proc. of the STC "Actual issues of technical support development in modern conditions"]. St. Petersburg: VA MTO, 2018. Vol. 7. Pp. 162–169. (In Rus)
8. Fedorov V.G., Starodubtsev Yu. I., Begaev A.N. Methodology for assessing the controllability of a fragment of a public communication network taking into account the influence of multiple control centers and destructive program impacts. *Voprosy kiberbezopasnosti* [Cybersecurity issues]. 2017. No. 4 (22). Pp. 32–39. (In Rus)
9. Komornikov P.M., Morozov R.V., Fatyanova E.V. O podhodah v ocenke nadezhnosti sistemy "operator – apparatno-programmnye sredstva svjazi" [On approaches in assessing the reliability of the system "operator-hardware-software communication tools"]. *Sbornik trudov III Mezhvuzovskoj nauchno-prakticheskoj konferencii "Problemy tehnicheskogo obespechenija vojsk v sovremennyh uslovijah"* [Proc. of the III Interuniversity scientific and practical conference "Problems of technical support of troops in modern conditions"]. St. Petersburg: VAS, 2018. Vol. 1. Pp. 303–307. (In Rus)
10. Evsevichev D.A., Samokhvalov M.K. Avtomatizacija rascheta jergonomicheskih parametrov sredstv otobrazhenija informacii na rabochem meste aviadispetchera [Automatied calculation of ergonomic parameters of the information display means at the workplace of the air traffic controller]. *Informacionnye sistemy* [Information systems]. 2017. No. 3 (49). Pp. 70–78. (In Rus)
11. Aalipour M., Ayele Y.Z., Barabadi A. Human reliability assessment (HRA) in maintenance of production process: a case study. *International Journal of System Assurance Engineering and Management.* 2016. No. 7. Pp. 229–238. (In Rus)
12. Chernysheva O.N. Problemy normirovanija parametrov predmetnoj sredy i ee jergonomicheskaja ocenka i proektirovanie [Problems of normalizing the parameters of the subject environment and its ergonomic assessment and design]ю *Trudy Vtoroj mezhdunarodnoj nauchno-prakticheskoj konferencii "Chelovecheskij faktor v slozhnyh tehnicheskih sistemah i sredah"*. [Proc. of the Second International scientific and practical Conference "Human factor in complex technical systems and environments" (Ergo 2016)]. (St. Petersburg, Russia, 6–9 July 2016) Ed. by A.N. Anokhin, P.I. Paderno, S.F. Sergeev. St. Petersburg: Interregional Ergonomic Association, FSAOU DPO "PEIPK", Severnaya Zvezda, 2016. Pp. 83–86. (In Rus)
13. Starodubtsev Yu. I., Fedorov V.G. Sposob obnaruzhenija istochnika setevyh atak na avtomatizirovannye sistemy [The method of detecting the source of network attacks on automated systems]. *Problemy jekonomiki i upravlenija v torgovle i promyshlennosti* [Problems of economics and management in trade and industry]. 2016. No. 1 (13). Pp. 87–92. (In Rus)
14. Alyushin M.V., Talalaev A.A. Obespechenie nadezhnosti professional'noj dejatel'nosti jekspluatacionnogo i dispetcherskogo personala jelektrojenergetiki [Ensuring the reliability of professional activity of operational and dispatching personnel of electric power]. *Trudy Tret'ej Mezhdunarodnoj nauchno-prakticheskoj konferencii "Chelovecheskij faktor v slozhnyh tehnicheskih sistemah i sredah"* . [Proc. of the Third International Scientific and Practical Conference "The human factor in complex technical systems and environments" (Ergo-2018)]. (St. Petersburg, Russia, July 4–7, 2018) Ed. by A.N. Anokhin, A.A. Oboznov, P.I. Paderno, S.F. Sergeev. St. Petersburg: SPbGETU "LETI", Interregional Ergonomic Association, 2018. Pp. 306–314. (In Rus)
15. Bogomolov A.V., Zinkin V.N., Alyokhin M.D., Sviridyuk G.A., Keller A.V. Informacionno-logicheskoe modelirovanie sbora i obrabotki informacii pri ocenivanii funkcional'noj nadezhnosti operatora aviacionnyh jergaticheskih sistem upravlenija [Information-logical modeling of information collection and processing in assessing the functional reliability of the operator of aviation ergatic control systems]. *Trudy Tret'ej Mezhdunarodnoj nauchno-prakticheskoj konferencii "Chelovecheskij faktor v slozhnyh tehnicheskih sistemah i sredah"*. [Proc. of the Third International Scientific and Practical Conference "The human factor in complex technical systems and environments" (Ergo-2018)]. (St. Petersburg, Russia, July 4–7, 2018). Ed. by A.N. Anokhin, A.A. Oboznov, P.I. Paderno, S.F. Sergeev. St. Petersburg: SPbGETU "LETI", Interregional Ergonomic Association, 2018. Pp. 315–323. (In Rus)
16. Starodubtsev Yu. I., Chukarikov A.G., Korsunsky A.S., Fedorov V.G. Method of protecting infotelekommunikatsionnyh networks of critical objects from network computer attacks. *Avtomatizatsiya protsessov upravleniya* [Automation of control processes]. 2018. No. 1 (51). Pp. 14–19. (In Rus)

INFORMATION ABOUT AUTHOR:
Fedorova S. V., postgraduate student, S. M. Budyonny Military Academy of communications.

For citation: Fedorova S.V. Detection of a multi-criteria indicator of the quality of the graphical interface of the software and hardware communication complex. *H&ES Research*. 2021. Vol. 13. No. 3. Pp. 20–27. Doi: 10.36724/2409-5419-2021-13-3-20-27 (In Rus)

Doi: 10.36724/2409-5419-2021-13-3-28-35

ИССЛЕДОВАНИЕ ПОДХОДОВ ДЛЯ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ БЕСПРОВОДНОЙ СЕТИ С ПРИМЕНЕНИЕМ РАЗЛИЧНЫХ LDAP РЕШЕНИЙ

ДОКШИН
Александр Денисович[1]

КОВЦУР
Максим Михайлович[2]

ПРУДНИКОВ
Сергей Владимирович[3]

ТАРГОНСКАЯ
Алина Игоревна[4]

АННОТАЦИЯ

Введение: с каждым годом технология сетей семейства IEEE802.11 становится все более распространенной и популярной. Опираясь на возможные риски, ИТ-администраторы принимают меры для защиты своих организаций. Один из способов повышения информационной безопасности – использование IEEE802.1x для авторизации пользователей. **Цель исследования:** целью исследования является изучение различных LDAP решений для авторизации пользователей в беспроводной сети. **Результаты:** разработано три варианта централизованного решения для авторизации пользователей беспроводной сети на базе операционных систем: Windows Server, Ubuntu Linux и Astra Linux. При работе с Windows Server было выявлено, что для хранения учетных данных пользователей можно использовать LDAP базу данных Active Directory. Так же исследование показало, что если в сетевой инфраструктуре организации необходимо реализовывать сервер с использованием операционной системы Linux, то в качестве LDAP базы данных можно использовать FreeIPA базу данных, а роль RADIUS сервера необходимо доверить программному обеспечению FreeRADIUS. Преимущество данного подхода заключается в том, что все программное обеспечение необходимо для авторизации пользователей – является бесплатным. Несмотря на то, что Active Directory является самой популярной LDAP базой данных – FreeIPA удовлетворяет всем потребностям, которые появляются во время администрирования системы безопасности. **Практическая значимость:** каждое решение прошло нагрузочное тестирование и может быть внедрено в сетевую инфраструктуру организаций. **Обсуждение:** выбор операционной системы и LDAP базы данных для авторизации пользователей полностью зависит от требований организации, поэтому под каждое требование подойдет один из предложенных вариантов реализации.

КЛЮЧЕВЫЕ СЛОВА: WiFi; LDAP; Active Directory; аутентификация; RADIUS.

Сведения об авторах:
[1]студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А.Бонч-Бруевича, г. Санкт-Петербург, Россия, a.dokshin007@gmail.com

[2]к.т.н., доцент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А.Бонч-Бруевича, г. Санкт-Петербург, Россия, maxkovzur@mail.ru

[3]старший преподаватель Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А.Бонч-Бруевича, г. Санкт-Петербург, Россия, prud2000@mail.ru

[4]студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А.Бонч-Бруевича, г. Санкт-Петербург, Россия, Targonskaya.ai@gmail.com

Для цитирования: *Докшин А.Д., Ковцур М.М., Прудников С.В., Таргонская А.И.* Исследование подходов для аутентификации пользователей беспроводной сети с применением различных LDAP решений // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13. № 3. С. 28–35. Doi: 10.36724/2409-5419-2021-13-3-28-35

Ведение

На данный момент беспроводная сеть является объектом постоянного внимания. Сегодня трудно представить современную инфраструктуру без внедрения беспроводных сетей, однако из-за высокой популярности беспроводных сетей необходимо уделять особое внимание информационной безопасности этих решений. Системные администраторы и IT-директора признают, что небезопасные сети семейства IEEE802.11 являются одним из общих векторов атаки [1].

Некоторые беспроводные сети защищены с помощью одного общего SSID и парольной фразы. Данный режим получил название PSK или режим предустановленного ключа аутентификации. Однако такой подход является небезопасным и неэффективным, если речь заходит о предоставлении доступа к беспроводной сети организации. Если общий SSID или парольная фраза состоят из большого количества символов, то велика вероятность, что они попадут в открытые источники [2]. Любой желающий может увидеть эту информацию. В некоторых случаях сигнал Wi-Fi достигает соседнего здания, парковки или тротуара. Таким образом, помимо угроз безопасности, защита сетей Wi-Fi с помощью парольных фраз также малоэффективна. В случае смены персонала в организации, администраторам приходится менять пароли, из-за чего могут возникнуть дополнительные сложности [3].

Решение данной проблемы заключается в аутентификации пользователя с использованием подхода IEEE802.1x при подключении к сети. Такой подход устраняет общую парольную фразу и гарантирует, что администратору не придется менять пароль каждый раз, когда сотрудник покидает организацию. В этом случае каждый пользователь имеет свои учетные данные для аутентификации. Такой режим получил название Enterprise или WPA2/WPA3 — Enterprise [4].

В данном исследовании описывается разработка наиболее эффективного подхода для авторизации пользователей Wi-Fi сети, применяя подход IEEE802.1x с внедрением LDAP баз данных. В ходе исследования будут представлены различные методы аутентификации пользователей на основе операционных систем (ОС) Windows и Linux. Уникальность данных методов заключается в том, что они позволяют компаниям отказаться от готовых коммерческих решений и сократить издержки.

Для анализа информационной безопасности IEEE802.11 исследованы актуальные проблемы в области беспроводных сетей, проведен обзор последних научных статей. Компания Microsoft проводила исследования с WLAN. Были проверены различные организации, в которых используются беспроводные сети. Анализ и статистика дали возможность понять, что существуют трудности в развертывании, управлении и безопасности корпоративных WLAN сетей. Согласно работе [5], можно сделать вывод о том, что систему безопасности многих компаний необходимо улучшать. Например, тот факт, что при подключении к беспроводной сети у пользователя запрашивалась только парольная фраза, весьма удивил исследователей.

Реализовать атаки на беспроводную сеть Wi-Fi можно различными способами. Атака типа “подслушивание”, может быть отнесена к категории особо опасных, так как злоумышленник может пассивно отслеживать трафик беспроводной сети и в нужный ему момент перехватить конфиденциальную информацию [6]. Атаки типа «фишинг (fishing)», позволяют злоумышленнику проникнуть в сеть путём создания дополнительной точки доступа. При этом рядовой пользователь не сможет определить, что точка доступа, к которой он подключается, заведомо создана злоумышленником [7]. Проблема заключается в том, что пользователь может передать секретный пароль злоумышленнику. Таким образом, данные уязвимости несут большой ущерб как коммерческой, так и конфиденциальной информации.

Централизованное хранение учетных данных

Хранилище идентификаторов пользователей относится к объекту, в котором хранятся имена пользователей и пароли. В большинстве случаев это сервер LDAP. Практически любой сервер RADIUS отправляет запрос LDAP базе данных для проверки каждого пользователя, который должен быть авторизован [8]. При использовании LDAP есть несколько предостережений, особенно в отношении того, как хешируются пароли на сервере LDAP. Если пароли не хранятся в виде открытого текста или хеша NTLM, то в этом случае необходимо выбирать методы EAP [9].

Разработка надежной сети WPA-Enterprise требует дополнительных условий, а именно наличия центра сертификации и беспрепятственного распространение сертификатов среди пользователей [10].

LDAP определяется как стандарт для каталогов, содержащих подробную информацию об учетных записях пользователей. Каталоги также могут содержать другие структурированные данные. Но для аутентификации пользователей в беспроводной сети можно ограничиться хранением учетных записей пользователей [11].

До LDAP службы каталогов разрабатывались телекоммуникационной отраслью для отслеживания клиентов и рассматривались как компьютеризированные телефонные книги. Первый стандарт X.500 был разработан Международным Союзом Электросвязи (МСЭ) в 1988 году.

LDAP был разработан в 1993 году в Мичиганском университете как простой способ доступа к первым каталогам X.500, которые располагались на серверах и обме-

нивались данными с клиентами по более сложному протоколу. LDAP должен был сделать взаимодействие более «легким», как подразумевается буквой «L» в LDAP [12].

Два года спустя следующая версия LDAPv2 была выпущена в серии из трех RFC. LDAPv2 устранила зависимость от X.500, в том числе изменив сетевое соединение с Open Standards Intercommunication (OSI) на более гибкую модель TCP / IP. Такой шаг сделал протокол более совместимым для интернет-коммуникаций [13].

Затем, в 1997 году появился LDAPv3, в котором улучшена поддержка каталогов, не основанных на X.500. Создан формат для URL-адресов LDAP, добавлены функции безопасности, такие, как аутентификация и расширения для TLS и SSL [14].

LDAP база данных предназначена для хранения каталогов. Данные LDAP структурированы и иерархичны. Структура определяется «схемами», которые описывают типы объектов, которые может хранить база данных, включая список всех их возможных атрибутов. Синтаксис, используемый для ссылки на конкретный объект в базе данных, основан на этой структуре. В наиболее распространенном случае, использование сервера LDAP позволяет централизовать управление учетными записями пользователей и соответствующими разрешениями. LDAP уникальным делает его древовидная структура, объединяющая пользователей в иерархии групп [15]. Каждый пользователь — это запись со своим уникальным идентификатором или отличительным именем (DN). Каждое DN имеет ряд атрибутов о пользователе, что позволяет зеркально отразить элементы управления доступом для пользователей в дереве каталогов. DN является доступным для объектно-ориентированных языков программирования. DN также может содержать информацию о URL, что делает его доступным через Интернет [16].

Способность LDAP объединяться с объектно-ориентированными языками программирования и DNS делает его идеальным для работы в Интернете. Он также составляет основу других интернет-протоколов, таких, как XML Enabled Directory (XED) и язык разметки службы каталогов (DSML) [17].

Древовидная структура LDAP вдохновила Microsoft на аналогичный подход в Active Directory, и с тех пор компания взяла на себя поддержку LDAP. Так Active Directory в Windows Server 2000 была только LDAP-совместимой, но уже в Windows Server Microsoft расширила поддержку LDAP и включила LDAP API в SDK платформы Microsoft Developer Network (MSDN).

Помимо Microsoft, LDAP поддерживается в продуктах от таких крупных компаний, как Sun Microsystems, Inc., IBM Corp., Hewlett-Packard Company, Novell Inc., Red Hat Inc., Oracle Corp., Apple Inc. и Siemens AG. Каждая из этих компаний предлагает службы каталогов, которые поддерживают LDAP [18].

Будущее LDAP заключается в расширении версии LDAPv3. В число последних улучшений, добавленных поставщиками, входят обновления графического интерфейса управления, упрощающие изменение пользователей и их атрибутов. В Windows Server Microsoft добавила службы безопасности LDAP и службы динамических каталогов, которые уже были в LDAPv3, но не отсутствовали в Active Directory.

Гибкость LDAP, масштабируемость и способность работать с новыми технологиями поддерживает популярность LDAP, который остается ядром многих служб каталогов сегодня.

Серверы каталогов LDAP часто используются в качестве хранилища для аутентификационных данных пользователей в различных системах, а также часто используются для хранения конфиденциальной информации, такой, как пароли и другие данные учетных записей. Информационная безопасность является важным аспектом большинства серверов каталогов и включает в себя множество функций политики паролей, поддержку различных типов аутентификации через SASL (простой уровень аутентификации и безопасности), возможность двухфакторных авторизаций.

Как правило, серверы каталогов предоставляют поддержку для детализированных элементов управления, ограничивающих доступ к записям, атрибутам и значениям для каждого отдельного пользователя.

Разработка централизованного решения для авторизации пользователей на базе операционной системы Windows

В данном решении для авторизации пользователей используется LDAP база данных Active Directory (AD), которая организует и защищает все ресурсы организации на Windows Server, включая пользователей, принтеры и общие файловые ресурсы. AD предоставляет администраторам инструмент, необходимый для того, чтобы у каждого пользователя или группы были соответствующие права на использование определенных ресурсов [19].

Active Directory, благодаря удобному графическому интерфейсу, пользуется популярностью у системных администраторов и дает возможность быстро менять привилегии для каждого пользователя, добавлять и удалять пользователей. Основой Active Directory являются доменные службы, которые хранят информацию о каталоге и обрабатывают взаимодействие пользователя с доменом. AD проверяет доступ, когда пользователь входит в устройство или пытается подключиться к серверу по сети, а также контролирует, какие пользователи имеют доступ к каждому ресурсу. При этом аутентификация поль-

зователей проводится с использованием протокола LDAP. Базы данных, поддерживающие этот протокол, часто применяют для централизованного хранения пользовательских идентификаторов [20].

Для установки LDAP базы данных Active Directory в Windows Server необходимо добавить роль сервера "Доменные службы Active Directory", после чего создать группу, пользователи которой смогут проходить авторизацию при подключении к беспроводной сети. Структурная схема авторизации при помощи LDAP базы данных Active Directory представлена на (рис. 1).

Эксперимент показал, что авторизация пользователей, учетные данные которых хранятся в LDAP базе данных проходит успешно, а значит Active Directory полностью подходит для хранения учетных данных.

Разработка централизованного решения для авторизации пользователей на базе операционной системы семейства Linux

В данном подходе будет использоваться LDAP база данных FreeIPA, за авторизацию и аутентификацию данных в этом решении отвечает программное обеспечение FreeRADIUS [21]. Программное обеспечение FreeIPA включает в себя LDAP базу данных. Загрузка программного обеспечения осуществляется бесплатно. Преимуществом является то, что помимо взаимодействия в консоли, FreeIPA имеет удобный графический интерфейс, что позволяет администраторам комфортно взаимодействовать с базой данных [22]. Также интерфейс и функционал аналогичен Active Directory. Помимо схожего интерфейса, FreeIPA возможно использовать совместно с Active Directory.

FreeIPA — это проект с открытым исходным кодом, спонсируемый Red Hat. Его целью является предоставление легко управляемого пакета Identity, Policy and Audit (IPA), в первую очередь предназначенного для систем Linux. FreeIPA легок в установке и позволяет улучшить информационную безопасность, а также хранит данные о всех пользователях, которым разрешено авторизоваться в сети [23].

Для установки FreeIPA нужно воспользоваться менеджером пакетов. Инсталляция в системе Linux Ubuntu производится при помощи apt (Advanced Packaging Tool) из официального хранилища.

Программное обеспечение FreeIPA поддерживает графический интерфейс, воспользоваться которым можно, если перейти в браузер и прописать в адресной строке доменное имя компьютера. Далее необходимо авторизоваться в LDAP базе данных. Для входа необходимо указать имя пользователя — admin, пароль, указанный при настройке FreeIPA. В графическом интерфейсе можно добавлять, удалять и привязывать к учетным данным привилегии. Для удобства есть возможность создать определенную группу политик, которым будут следовать пользователи, принадлежащие этой группе. Структурная

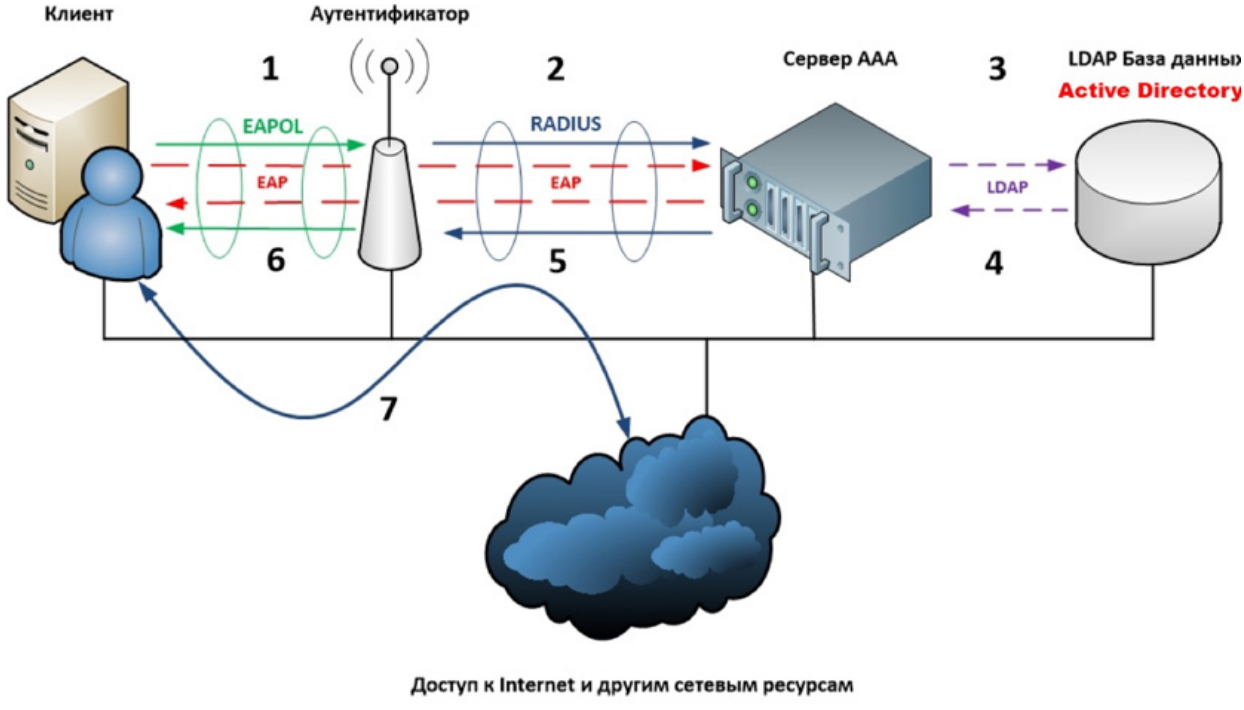


Рис. 1. Реализация RADIUS авторизации на базе операционной системы Windows Server

схема авторизации при помощи LDAP базы данных FreeIPA представлена на (рис. 2).

После настройки всего оборудования, эксперимент показал, что пользователи без труда могут пройти авторизацию, а значит LDAP база данных FreeIPA полностью подходит для хранения учетных данных пользователей для беспроводных клиентов.

Настройка сервера аутентификации на базе Astra Linux

После успешного внедрения сервера для аутентификации и авторизации пользователей на базе Windows и Linux Ubuntu появляется потребность осуществить весь реализованный функционал в операционной системе российского производства.

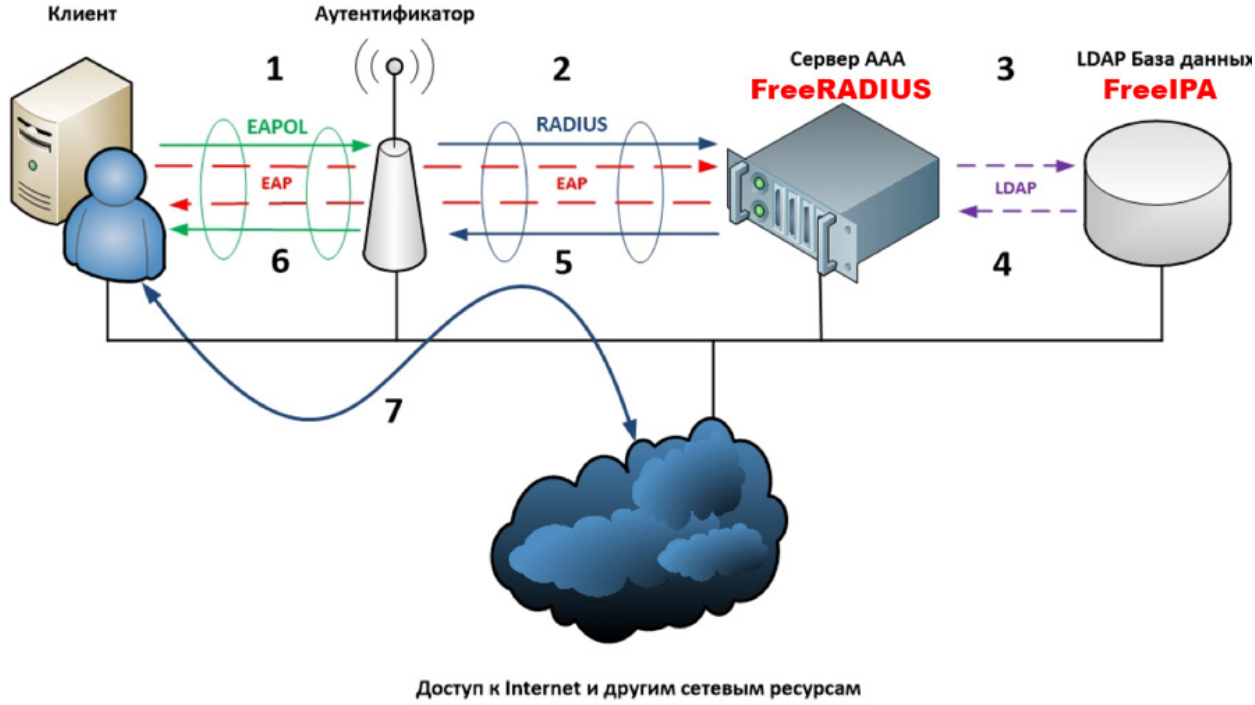


Рис. 2. Реализация RADIUS авторизации на базе операционной системы семейства Linux

Astra Linux — компьютерная операционная система, изначально разработанная для использования в вооруженных силах Российской Федерации. Данная операционная система устанавливается во всех организациях, связанных с безопасностью страны. Astra Linux получил сертификацию Министерства обороны России и Федеральной службы безопасности (ФСБ) [24].

Данная операционная система также доступна для домашнего и корпоративного использования. Преимущество внедрения Astra Linux заключается в том, что это позволяет полностью отказаться от ОС зарубежного производства [25].

В реализации сервера для авторизации в качестве LDAP базы данных используется FreeIPA, роль RADIUS сервера играет программное обеспечение FreeRADIUS.

Процесс реализации LDAP базы данных на операционной системе Astra Linux точно такой же, как и на Linux Ubuntu, поэтому весь функционал, ОС Ubuntu — будет доступен в Astra Linux. После успешного внедрения FreeIPA пользователю становится доступным графический интерфейс, в которой возможно зайти при помощи браузера.

Таким образом, на практике реализован сервер для аутентификации и авторизации пользователей на базе ОС российского производства. Данный метод позволяет полностью отказаться от систем зарубежных разработчиков.

Заключение

Для защиты от основных атак на беспроводные сети была представлена концепция аутентификации и авторизации пользователей при помощи различных LDAP решений. Исследование показало, что RADIUS-сервер может быть реализован на базе ОС Windows Server и систем семейства Linux. Реализация на базе ОС Astra Linux решает вопрос импортозамещения. Данное решение показало хорошие результаты, в связи с чем может быть внедрено в систему безопасности беспроводной сети предприятия.

Дальнейшими задачами является реализация тестирования для выявления критической нагрузки сервера при авторизации пользователей и на основе этого подбор необходимых характеристик оборудования для повышения порога пиковой нагрузки на сервер.

Литература

1. *Штеренберг С.И., Стародубцев И.В., Шашкин В.С.* Разработка комплекса мер для защиты предприятия от фишинговых атак // Защита информации. Инсайд. 2020. № 2 (92). С. 24–31.

2. *Киреева Е.В.* Методы защиты информации от несанкционированного доступа в wifi сетях // Мировая наука. 2019. № 12 (33). С. 200–202.

3. *Докшин А.Д., Даньшина А.В., Ковцур М.М., Юркин Д.В.* Исследование подходов авторизации пользователей беспроводной сети на основе LDAP // Аллея Науки. 2020. Т. 1. № 3 (42). С. 758–761.

4. *Ковцур М.М., Симанов М.С.* Анализ особенностей организации авторизации пользователей в сетях коллективного доступа стандарта IEEE802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019): сборник научных статей VIII Международной научно-технической и научно-методической конференции. 2019. С. 537–541.

5. *Ломако А.Г., Овчаров В.А., Акулов С.А., Коротков В.С.* Механизмы реализации типовых атак на компоненты беспроводных сетей передачи данных // The 2017 Symposium on Cybersecurity of the Digital Economy (CDE'17). Book of Abstracts. 2017. С. 249–254.

6. *Сахаров Д.В., Красов А.В., Ушаков И.А., Бирих Э.В.* Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе IPv6 // Защита информации. Инсайд. 2020. № 1 (91). С. 51–57.

7. *Shterenberg S.I., Poltavtseva M.A.* A distributed intrusion detection system with protection from an internal intruder // Automatic Control and Computer Sciences. 2018. Vol. 52. No. 8. Pp. 945–953.

8. *Красов А.В., Косов Н.А., Холоденко В.Ю.* Исследование методов провижининга безопасной сети на мультивендорном оборудовании с использованием средств автоматизированной конфигурации // Colloquium-journal. 2019. № 13–2 (37). С. 243–247.

9. *Полищук С.* Новый подход к сегментации сети и его ценность для бизнеса // Журнал сетевых решений LAN. 2017. № 1–2. С. 37–42.

10. *Красов А.В., Сахаров Д.В., Ушаков И.А., Лосин Е.П.* Обеспечение безопасности передачи multicast-трафика в ip-сетях // Защита информации. Инсайд. 2017. № 3 (75). С. 34–42.

11. *Sharikov P.I., Krasov AV., Gelfand A.M., Kosov N.A.* Research of the possibility of hidden embedding of a digital watermark using practical methods of channel steganography // Intelligent Distributed Computing XIII 2019. Pp. 203–209.

12. *Цветков А.Ю.* Исследование существующих механизмов защиты операционных систем семейства Linux // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018) VII Международная научно-техническая и научно-методическая конференция: Сборник научных статей / Под редакцией С.В. Бачевского. 2018. С. 657–662.

13. Iskhakov A., Meshcheryakov R., Ekhlakov Yu. The internet of things in the security industry // Interactive systems: Problems of Human-Computer Interaction. Collection of scientific papers. 2017. Pp. 161–168.

14. *Стародубцев Ю.И., Закалкин П.В., Иванов С.А., Добрышин М.М.* Способ защиты серверов услуг сети связи от компьютерных атак // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2020. № 9–10 (147–148). С. 63–67.

15. *Александров Е.С., Иванов Г.Н., Ковцур М.М.* Анализ механизмов защиты WI-FI сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018) VII Международная научно-техническая и научно-методическая конференция: Сборник научных статей / Под редакцией С.В. Бачевского. 2018. С. 657–662.

16. *Сахаров Д.В., Красов А.В., Ушаков И.А., Бирих Э.В.* Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе IPv6 // Защита информации. Инсайд. 2020. № 1 (91). С. 51–57.

17. *Темченко В.И., Цветков А.Ю.* Проектирование модели информационной безопасности в операционной системе // Актуальные проблемы инфотелекоммуникаций в науке и образование. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2019. С. 740–745.

18. *Багомедова А.Р., Ушаков И.А., Цветков А.Ю.* Разработка методов проверки соответствия серверов виртуализации требованиям безопасности согласно стандарту ГОСТ Р 56938–2016 // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018): сборник статей VII Международной научно-технической и научно-методической конференции. 2018. С. 58–63.

19. *Akbashev R.R.* The analysis of information security problems in the computer network, which is connected to the internet // Information Technology. Problems and Solutions: Proceedings of the International scientific-practical conference. 2017. № 1 (4). Pp. 295–298.

20. *Basan A., Basan E., Makarevich O., Teterevyatnikov S.* Research of influence of the attacks on the group of mobile wireless network nodes // Integrating Research Agendas and Devising Joint Challenges. International Multidisciplinary Symposium ICT Research in Russian Federation and Europe. 2018. Pp. 20–28.

21. *Makashov A.* The network layer model of the wireless sensor network acting under the influence of interferences // 2019 3rd School on Dynamics of Complex Networks and their Application in Intellectual Robotics, DCNAIR2019. No. 3. 2019. Pp. 116–118.

22. *Ушаков И.А.* Обнаружение инсайдеров в корпоративной компьютерной сети на основе технологий анализа больших данных // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2019. № 4. С. 38–43.

23. *Котенко И.В., Кулешов А.А., Ушаков И.А.* Система сбора, хранения и обработки информации и событий безопасности на основе средств Elastic stack // Труды СПИИРАН. 2017. № 5 (54). С. 5–34.

24. *Штеренберг С.И., Полтавцева М.А.* Распределенная система обнаружения вторжений с защитой от внутреннего нарушителя // Проблемы информационной безопасности. Компьютерные системы. 2018. № 2. С. 59–68.

25. *Суворов А.М., Цветков А.Ю.* Исследование атак типа переполнение буфера в 64-х разрядных unix подобных операционных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. 2018. С. 570–573.

RESEARCH OF APPROACHES FOR AUTHENTICATION OF WIRELESS NETWORK USERS USING VARIOUS LDAP SOLUTIONS

ALEXANDR D.DOKSHIN

St. Petersburg, Russia, a.dokshin007@gmail.com

MAXIM M. KOVTSUR

St. Petersburg, Russia, maxkovzur@mail.ru

SERGEI V. PRUDNIKOV

St. Petersburg, Russia, prud2000@mail.ru

ALINA I. TARGONSKAYA

St. Petersburg, Russia, targonskaya.ai@gmail.com

KEYWORDS: economic model, large technical system; life cycle stages; system cost estimate; simulation modeling of system development; serial production of products; effective management decisions.

ABSTRACT

Intoduction: every year, the technology of the IEEE802.11 family of networks is becoming more widespread and popular. Based on the possible risks, IT administrators take measures to protect their organizations. One of the ways to improve information security is to use IEEE802.1 x for user authorization. **Purpose:** the purpose of the study is to study various LDAP solutions for user authorization in a wireless network. **Results:** three variants of the centralized solution for authorization of users of a wireless network on the basis of operating systems are developed: Windows Server, Ubuntu Linux, and Astra Linux. When working with Windows Server, it was found that you can use the Active Directory LDAP database to store user credentials. The study also showed that if the network infrastructure of the organization needs to implement a server using the Linux operating system, then the FreeIPA database can be used as an LDAP database, and the role of the RADIUS server must be entrusted to the FreeRADIUS software. The advantage of this approach is that all the software required for user authorization is free. Despite the fact that Active Directory is the most popular LDAP database-FreeIPA meets all the needs that arise during security administration. **Practical relevance:** each solution has passed load testing and can be implemented in the network infrastructure of organizations. **Discussion:** the choice of operating system and LDAP database for user authorization completely depends on the requirements of the organization, so one of the proposed implementation options will fit each requirement.

REFERENCES

1. Shterenberg S.I., Starodubtsev I.V., Shashkin V.S. Development of a set of measures to protect an enterprise from phishing attacks. *Zaschita informacii. Insaid.* 2020. No. 2 (92). Pp. 24–31. (In Rus)
2. Kireeva E.V. Methods for protecting information from unauthorized access in wifi networks. *Mirovaya nauka* [World Science]. 2019. No. 12. Pp 200–202. (In Rus)
3. Dokshin A.D., Danshina A.V., Kovtsur M.M., Yurkin D.V. Investigation of LDAP-based wireless network user authorization approaches. *Alleya Nauki* [Alley of Science]. 2020. T. 1. № 3 (42). Pp. 758–761. (In Rus)
4. Kovtsur M.M., Simanov M.S. Analiz osobennostei organizacii avtorizacii polzovatelei v setyah kollektivnogo dostupa standarta IEEE802.11 [Analysis of the features of the organization of user authorization in the networks of collective access of the IEEE802.11 standard]. *Aktualnie problemi infotelekommunikacii v nauke i obrazovanii APINO 2019: Sbornik nauchnih statei VIII Mejdunarodnoi nauchno_tehnicheskoi i nauchno_metodicheskoi konferencii* [Actual problems of infotelecommunications in science and education (APINO 2019). Collection of scientific articles of the VIII International Scientific-Technical and Scientific-methodological Conference]. 2019. Pp. 537–541. (In Rus)
5. Lomako A.G., Ovcharov V.A., Akulov S.A., Korotkov V.S. Mehanizmi realizacii tipovih atak na komponenti besprovodnih setei peredachi dannih [Mechanisms for implementing typical attacks on components of wireless data networks]. *The 2017 Symposium on Cybersecurity of the Digital Economy (CDE'17). Book of Abstracts.* 2017. Pp. 249–254. (In Rus)
6. Saharov D.V., Krasov A.V., Ushakov I.A., Birih E.V. Modeling a secure, scalable enterprise network with IPv6-based dynamic routing. *Zaschita informacii. Insaid* [Information security. Inside view]. 2020. No. 1 (91). Pp. 51–57. (In Rus)
7. Shterenberg S.I., Poltavtseva M.A. A distributed intrusion detection system with protection from an internal intruder. *Automatic Control and Computer Sciences.* 2018. Vol. 52. No. 8. Pp. 945–953.
8. Krasov A.V., Kosov N.A., Holodenko V. Yu. Research of methods of secure network provisioning on multi-vendor equipment using automated configuration tools. *Colloquium-journal.* 2019. No. 13–2 (37). Pp. 243–247. (In Rus)
9. Polishchuk C. A new approach to network segmentation and its business value. *Jurnal setevih reshenii LAN* [Network Solutions Journal LAN]. 2017. No. 1–2. Pp. 37–42. (In Rus)
10. Krasov A.V., Saharov D.V., Ushakov I.A., Losin E.P. Ensuring the secu-

rity of multicast traffic transmission in IP networks. *Zaschita informacii. Insaid* [Information security. Inside view]. 2017. № 3 (75). Pp. 34–42. (In Rus)
11. Sharikov P.I., Krasov AV., Gelfand A.M., Kosov N.A. Research of the possibility of hidden embedding of a digital watermark using practical methods of channel steganography. *Intelligent Distributed Computing XIII*. 2019. Pp. 203–209.
12. Tsvetkov A. Yu. Issledovanie suschestvuyuschih mehanizmov zaschiti operacionnih sistem semeistva Linux [Research of the existing mechanisms of protection of operating systems of the Linux family]. *Aktualnie problemi infotelekommunikacii v nauke i obrazovanii APINO 2018, VII Mejdunarodnaya nauchno_tehnicheskaya i nauchno_metodicheskaya konferenciya. Sbornik nauchnih statei* [Actual problems of infotelecommunications in science and education (APINO 2018) VII International Scientific-technical and scientific-methodological Conference. Collection of scientific articles. Edited by S.V. Bachevsky]. 2018. Pp. 657–662. (In Rus)
13. Iskhakov A., Meshcheryakov R., Ekhlakov Yu. The internet of things in the security industry. *Interactive systems: Problems of Human-Computer Interaction. Collection of scientific papers.* 2017. Pp. 161–168.
14. Starodubcev Yu.I., Zakalkin P.V., Ivanov S.A., Dobrishin M.M. A method for protecting communication network service servers from computer attacks. *Voprosi oboronnoi tehniki. Seriya 16 Tehnicheskie sredstva protivodeistviya terrorizmu* [Questions of defense equipment. Series 16: Technical means of countering terrorism]. 2020. No. 9–10 (147–148). Pp. 63–67. (In Rus)
15. Aleksandrov E.S., Ivanov G.N., Kovcur M.M. Analiz mehanizmov zaschiti WI_FI setei [Analysis of WI-FI network protection mechanisms]. *Aktualnie problemi infotelekommunikacii v nauke i obrazovanii APINO 2018. VII Mejdunarodnaya nauchno_tehnicheskaya i nauchno_metodicheskaya konferenciya* [Actual problems of infotelecommunications in science and education (APINO 2018). Proc. of the VII International Scientific-technical and scientific-methodological Conference]. St. Petersburg, 2018. Pp 657–662. (In Rus)
16. Saharov D.V._ Krasov A.V._ Ushakov I.A._ Birih E.V. Modeling a secure, scalable enterprise network with IPv6-based dynamic routing. *Zaschita informacii. Insaid* [Information security. Inside view]. 2020. No. 1 (91). Pp. 51–57. (In Rus)
17. Timchenko V.I., Tsvetkov A. Yu. Proektirovanie modeli informacionnoi bezopasnosti v operacionnoi sisteme [Designing an information security model in an operating system]. *Aktualnie problemi infotelekommunikacii v nauke i obrazovanie. VIII Mejdunarodnaya nauchno_tehnicheskaya i nauchno_metodicheskaya konferenciya* [Actual problems of infotelecommunications in science and education. VIII International Scientific-technical and scientific-methodological Conference]. St. Petersburg: SPbGUT, 2019. Pp. 740–745. (In Rus)
18. Bagomedova A.R., Ushakov I.A., Tsvetkov A. Yu. Razrabotka metodov proverki sootvetstviya serverov virtualizacii trebovaniyam bezopasnosti soglasno standartu GOST R56938_2016 [Development of methods for verifying the compliance of virtualization servers with security requirements in accordance with GOST R56938–2016]. *Aktualnie problemi infotelekommunikacii v nauke i obrazovanii _APINO 2018. Sbornik statei VII Mejdunarodnoi nauchno_tehnicheskoi i nauchno_metodicheskoi konferencii* [Actual problems of infotelecommunications in science and education APINA 2018. Collection of articles of the VII International nauchno_tehnicheskoi i nauchno_metodicheskoi konferencii.]. St. Petersburg, 2018. Pp. 58–63. (In Rus)
19. Akbashev R.R. The analysis of information security problems in the computer network, which is connected to the internet. *Information Technology. Problems and Solutions: Proceedings of the International scientific-practical conference.* 2017. No. 1 (4). Pp. 295–298.
20. Basan A., Basan E., Makarevich O., Teterevyatnikov S. Research of influence of the attacks on the group of mobile wireless network nodes. *Integrating Research Agendas and Devising Joint Challenges. International Multidisciplinary Symposium ICT Research in Russian Federation and Europe*. 2018. Pp. 20–28.
21. Makashov A. The network layer model of the wireless sensor network acting under the influence of interferences. *2019 3rd School on Dynamics of Complex Networks and their Application in Intellectual Robotics,* DCNAIR2019. No. 3. 2019. Pp. 116–118.
22. Ushakov I.A. Detection of insiders in the corporate computer network based on big data analysis technologies. *Vestnik Sankt_Peterburgskogo gosudarstvennogo universiteta tehnologii i dizaina. Seriya 1: Estestvennie i tehnicheskie nauki* [Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences]. 2019. No. 4. Pp. 38–43. (In Rus)
23. Kotenko I.V., Kuleshov A.A., Ushakov I.A. A system for collecting, storing and processing security information and events based on Elastic stack tools. *Trudi SPIIRAN* [Works of SPIIRAN]. 2017. No. 5 (54). Pp. 5–34. (In Rus)
24. Shterenberg S.I., Poltavtseva M.A. Distributed intrusion detection system with internal intruder protection. Problemi informacionnoi bezopasnosti. *Kompyuternie sistemi* [Problems of information security. Computer systems]. 2018. No. 2. Pp. 59–68. (In Rus)
25. Suvorov A.M., Tsvetkov A. Yu. Issledovanie atak tipa perepolnenie bufera v 64_h razryadnih unix podobnih operacionnih sistemah [Investigation of buffer overflow attacks in 64-bit unix-like operating systems]. *Aktualnie problemi infotelekommunikacii v nauke i obrazovanii APINO 2018. VII Mejdunarodnaya nauchno_tehnicheskaya i nauchno_metodich*eskaya konferenciya [Actual problems of infotelecommunications in science and education (APINO 2018). VII International Scientific-technical and scientific-methodological Conference]. St. Petersburg. 2018. Pp. 570–573. (In Rus)

INFORMATION ABOUT AUTHORS:

Dokshin A.D., student of The Bonch-Bruevich Saint-Petersburg State University of Telecommunications;
Kovtsur M.M., PhD, docent of The Bonch-Bruevich Saint-Petersburg State University of Telecommunications;
Prudnikov S.V., Senior lecturer of The Bonch-Bruevich Saint-Petersburg State University of Telecommunications;
Targonskaya A.I., student of The Bonch-Bruevich Saint-Petersburg State University of Telecommunications.

For citation: Dokshin A.D., Kovtsur M.M., Prudnikov S.V., Targonskaya A.I. Research of approaches for authentication of wireless network users using various LDAP solutions. *H&ES Research*. 2021. Vol. 13. No. 3. Pp. 28–35. Doi: 10.36724/2409-5419-2021-13-3-28-35 (In Rus)

Doi: 10.36724/2409-5419-2021-13-3-36-47

МЕТОДИКА ФОРМИРОВАНИЯ АДАПТИВНОГО СЦЕНАРИЯ ДИАЛОГА ПРИ РЕШЕНИИ АВТОМАТИЗИРОВАННЫХ ЗАДАЧ УПРАВЛЕНИЯ НА РАБОЧЕМ МЕСТЕ КОМПЛЕКСА СРЕДСТВ АВТОМАТИЗАЦИИ ВОЕННОГО НАЗНАЧЕНИЯ

ЗЮЗИН
Алексей Владимирович[1]

КУРЧИДИС
Виктор Александрович[2]

МОРОЗОВ
Павел Андреевич[3]

АНОШИН
Роман Игоревич[4]

АННОТАЦИЯ

Введение: проведенный анализ показывает, что одним из наиболее предпочтительных направлений сокращения работного времени боевого расчета органа управления является применение диалогового режима взаимодействия между лицами боевого расчета и автоматизированным рабочим местом комплекса средств автоматизации на основе применения запросов на естественно-подобном языке. **Цель исследования:** целью исследования является определение сценария диалога адаптивного запросу лица боевого расчета при решении автоматизированных задач управления. **Методы**: Для достижения цели предлагается представить структуру диалога в виде множества взвешенных ориентированных графов диалога, что позволяет учитывать последовательность ввода данных при решении задач управления применяя методы определения компонент сильной связности и определения порядка шагов диалога внутри них на основе отношений межфреймовых связей. **Результаты:** использование представленного решения позволяет в процессе решения автоматизированных задач управления на естественно-подобном языке формировать сценарий диалога адаптивный запросу лица боевого расчета. Элементами новизны является формализованное представление структурных составляющих запроса лица боевого расчета органа управления на естественно-подобном языке предикатной моделью для учета изменений, вносимых в структуру взвешенного ориентированного директивного графа диалога. Множество условий после предикатно-предметной интерпретации и проверки на корректность значений представляются в виде пустого графа. Операция вычитания между взвешенным ориентированным директивным графом диалога и пустым графом позволяет сформировать множество результирующих шагов диалога и определить функцию перехода между ними. **Практическая значимость:** представленное решение предлагается реализовать в виде программного модуля диалоговой системы комплекса средств автоматизации военного назначения выполненного на языке программирования высокого уровня C/C++ с применением библиотеки QT. **Обсуждение:** реализация предлагаемого решения в виде кроссплатформенного программного модуля позволит интегрировать его в существующее специальное программное обеспечение средств автоматизации.

КЛЮЧЕВЫЕ СЛОВА: оперативность управления; задачи управления; естественно-языковое взаимодействие; продукционно-фреймовая модель; шаг диалога; граф диалога.

Сведения об авторах:
[1]д.т.н., профессор, заведующий кафедрой Ярославского высшего военного училища противовоздушной обороны, г. Ярославль, Россия, aleksey.zyuzin@mail.ru

[2]д.т.н., профессор, профессор Ярославского высшего военного училища противовоздушной обороны, г. Ярославль, Россия, idahmer2@yandex.ru

[3]к.т.н., доцент, докторант Ярославского высшего военного училища противовоздушной обороны, г. Ярославль, Россия, mpa24@mail.ru

[4]адъюнкт Ярославского высшего военного училища противовоздушной обороны, г. Ярославль, Россия, roman88an@gmail.com

Для цитирования: *Зюзин А.В., Курчидис В.А., Морозов П.А., Аношин Р.И.* Методика формирования адаптивного сценария диалога при решении автоматизированных задач управления на рабочем месте комплекса средств автоматизации военного назначения // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13. № 3. С. 36–47. Doi: 10.36724/2409-5419-2021-13-3-36-47

Введение

В настоящее время обеспечение оперативного управления силами и средствами в войсках ВКС, достижение обоснованности и оптимальности принимаемых решений, а также осуществления качественного планирования и контроля деятельности войск достигается путем применения автоматизированных систем управления (АСУ). Однако, опыт локальных войн и вооруженных конфликтов последних лет [1–5] показывает, что бурное развитие средств воздушно-космического нападения (СВКН), способов их боевого применения, а также модернизация существующего вооружения и военной техники вероятного противника влечет необходимость повышения эффективности АСУ.

В общем случае АСУ представляет собой совокупность личного состава, комплекса средств автоматизации (КСА) и средств связи, реализующая информационную технологию выполнения задач по обработке информации и управления. Одним из наиболее существенных показателей эффективности АСУ, который в большей степени влияет на реализацию боевых возможностей войск (сил) является оперативность, т.е. возможность системы реагировать на изменение обстановки [6]. Количественно оперативность оценивается работным временем $T_{раб}$ — временными затратами боевого расчета органа управления (БР ОУ) при решении поставленных перед ними задач. Чем меньше работное время, тем выше быстродействие системы и тем выше ее оперативность. Уменьшение составляющих работного времени без снижения качества решения задач управления является одним из важнейших направлений по повышению оперативности управления.

Основная часть

Анализ решаемых БР ОУ задач $Z_{БРОУ}$ показал, что он включает в себя широкий круг задач, часть из которых может быть формализована и решена автоматизировано $\tilde{Z} = \{\tilde{z}_1, \tilde{z}_2, ..., \tilde{z}_n\}$, другая — не формализуемая и входящие в ее состав задачи $\hat{Z} = \{\hat{z}_1, \hat{z}_2, ..., \hat{z}_m\}$ решаются БР ОУ с учетом их творческих замыслов и условий обстановки, т.е. неавтоматизированно. При этом время решения автоматизированных задач управления вносит существенный вклад в значение работного времени БР ОУ.

Отметим, что каждая автоматизированная задача управления $\tilde{z}_i \in \tilde{Z}$ может быть представлена как функция, зависящая от множества данных D_i поступающих от ЛБР данных D_i', вычислительных средств $\hat{D}_i$ и базы данных КСА $\bar{D}_i$.

В зависимости от количества данных, вводимых ЛБР, все автоматизированные задачи управления целесообразно разделить на унарные и полиадические. Под унарными задачами понимаются задачи в которых $|D_i'| = 1$, а под полиадическими — $|D_i'| > 1$.

Анализ направлений сокращения работного времени БР ОУ показывает, что наиболее предпочтительным из них является применение запросов на естественно-подобном языке [7–8]. Отметим, что в этом направлении известен ряд работ [9–13]. Однако подход, описанный в них, имеет ряд недостатков:

1. Подход применим исключительно для решения унарных задач управления.

2. В случае отсутствия необходимых данных в запросе ЛБР ОУ, а также в случае ошибки в значении этих данных задача управления не будет выполнена и система в большинстве случаев не сообщит об этом, а если и сообщит, то только формализованной квитанцией и ЛБР ОУ придется формировать запрос повторно, что в свою очередь приводит к значительному увеличению времени формирования оперативной информации.

3. Анализ порядка решения полиадических задач управления на АРМ КСА показывает, что количество данных, вводимых ЛБР ОУ для их решения может иметь достаточно большое значение, дополнительно к этому накладывается требование и к порядку ввода этих данных. Этот факт накладывает одно весьма значительное ограничение, которое заключается в том, что чем больше количество данных в запросе ЛБР ОУ на естественно-подобном языке, тем выше вероятность их некорректного ввода, что в свою очередь предъявляет очень жесткие требования для профессиональной подготовки ЛБР ОУ.

Данные недостатки сдерживают применение известного способа при решении полиадических задач управления, и обуславливают необходимость разработки нового способа, основанного на диалоговом режиме взаимодействия между ЛБР и АРМ КСА с возможностью перехвата инициативы. Решение проблемы организации такого диалогового взаимодействия предлагается осуществить на основе способа формирования адаптивного сценария диалога (рис. 1) включающего этапы:

- формирование множества взвешенных ориентированных директивных графов диалога;
- формирование адаптивной структуры диалога.

Задачей первого этапа работы предложенного способа является описание графовой модели диалога между лицами боевого расчета (ЛБР) и АРМ КСА. С целью выполнения данной задачи рассмотрим взаимодействие ЛБР и АРМ КСА как процесс достижения определенных согласованных целей путем обмена связанными сообщениями (высказываниями) и введем ряд необходимых понятий.

Все сообщения, которыми обмениваются участники диалога между собой образуют единую сложную конструкцию, называемую структурой диалога. Описание структуры диалога производится путем его декомпозиции на части, называемые шагами диалога $X = \{x_1, x_2, \ldots, x_n\}$ [14]. В общем случае под шагом диалога $x_i \in X$ понимается законченная процедура интерактивного взаимодействия ЛБР И АРМ КСА, представленная в виде пары «действие-реакция». Сообщение

активного участника диалога соответствует «действию», а пассивного — «реакции». Последовательность переходов между множеством шагов диалога необходимая для достижения поставленной цели называется сценарием диалога.

Формализация структуры диалога производится в виде графа диалога $G(X, F)$, где X — счетное множество шагов диалога, а F — функция отображения $F: X \to X \cup \varnothing$, в которой $x_j \in \{F(x_i)\}$, если существует шаг диалога, задаваемый траекторией $x_i \to x_j$, при этом данное отображение определяет на графе множество ориентированных ребер $U = \{u_1, u_2, \ldots, u_k\}$, $|U| = k$. Формализм в виде графа диалога $G(X, F)$ позволяет описать структуру диалога и множество его возможных сценариев в рамках дискретной математики и структур универсальных алгебр.

Существует три эквивалентных способа задания графа диалога: аналитический, введенный выше, геометрический и матричный. Геометрический способ задания графа диалога используется в качестве изобразительного, наглядного средства представления, при этом множество элементов X графа G (вершин) изображается кругами, а отображение F — стрелками (ребра графа). Для задания графа диалога в матричной форме используется квадратичная матрица смежности:

$$A(G) = \|a_{\alpha\beta}\| = \begin{Vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & & a_{2n} \\ \vdots & & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{Vmatrix}$$

элементы которой представляются нулями или единицами по следующему правилу: элемент $a_{\alpha\beta}$, стоящий на пересечении α-ой строки и β-го столбца, равен единице, если имеется ребро, соединяющее вершины x_α и x_β, и равен нулю в противном случае, т.е.

$$a_{\alpha\beta} = \begin{cases} 1, x_\beta \in F(x_\alpha); \\ 0, x_\beta \notin F(x_\alpha). \end{cases}$$

Подчеркнем, что в настоящее время диалоговое взаимодействие между ЛБР и АРМ КСА ограничено существующей информационной моделью отображения (ИМО), построенной на основе многоуровневого пользовательского меню [15, 16] (рис. 2). Такой способ взаимодействия характеризуется тем, что АРМ КСА предоставляет ЛБР для выполнения задачи управления четкую, заранее определенную последовательность кадров меню, тем самым лишая его свободы в выборе наиболее удобной для него очередности ввода данных, а также шага диалога с которого начинается взаимодействие — точки входа.

Организация диалогового взаимодействия между ЛБР и АРМ КСА на естественно-подобном языке снимает данное ограничение. Вершины графа диалога (рис. 3) $G(X, F)$ образующие два различных шага диалога (x_i, x_j), $x_i \in X$ и $x_j \in X$, при этом могут быть соединены ребрами в различных направлениях.

Последовательность действий, позволяющих сформировать множества взвешенных ориентированных директивных графов диалога представлена на рис. 4.

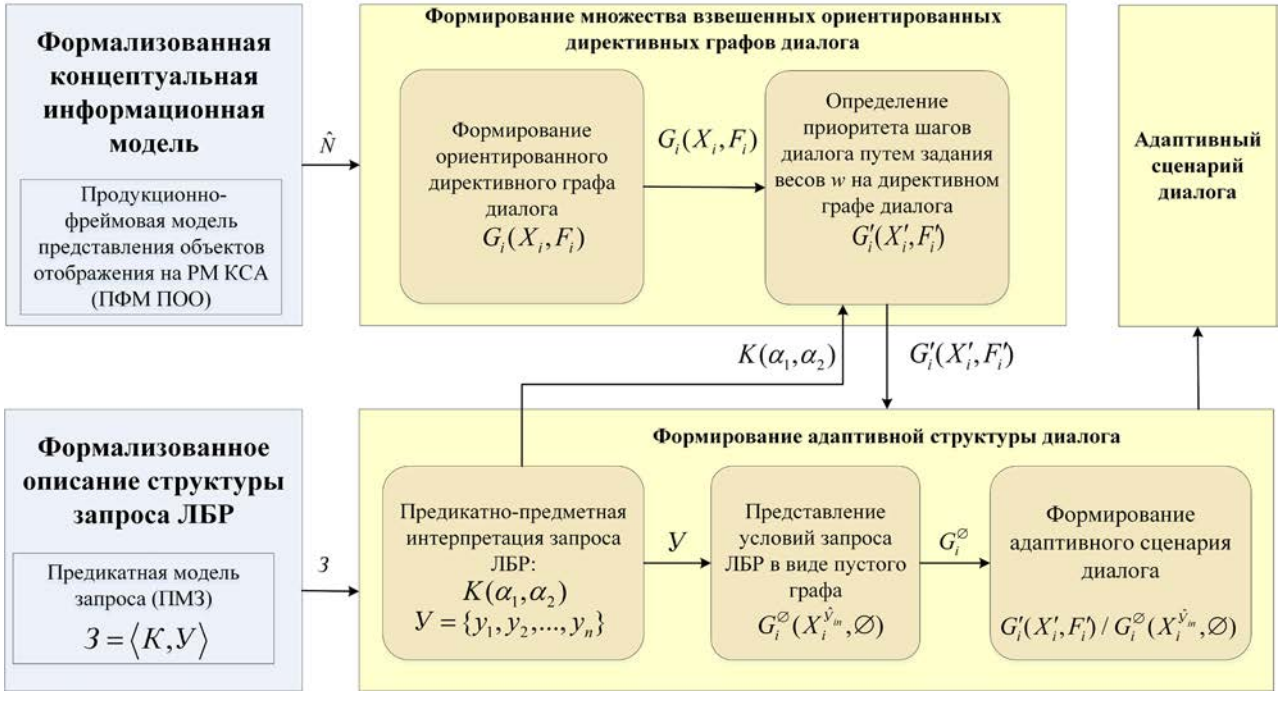


Рис. 1. Способ формирования адаптивного сценария диалога

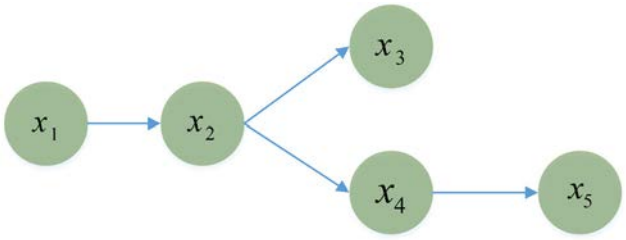


Рис. 2. Директивный граф диалога построенный по типу меню

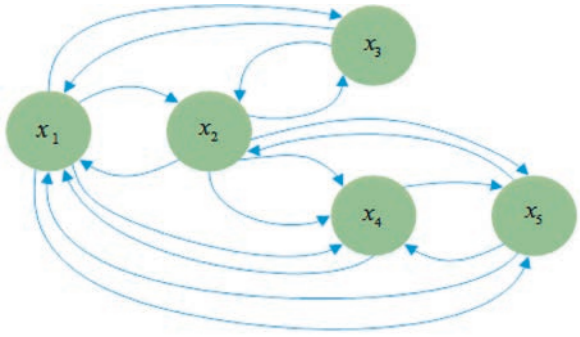


Рис. 3. Директивный граф диалога между ЛБР и АРМ КСА естественно-подобном языке

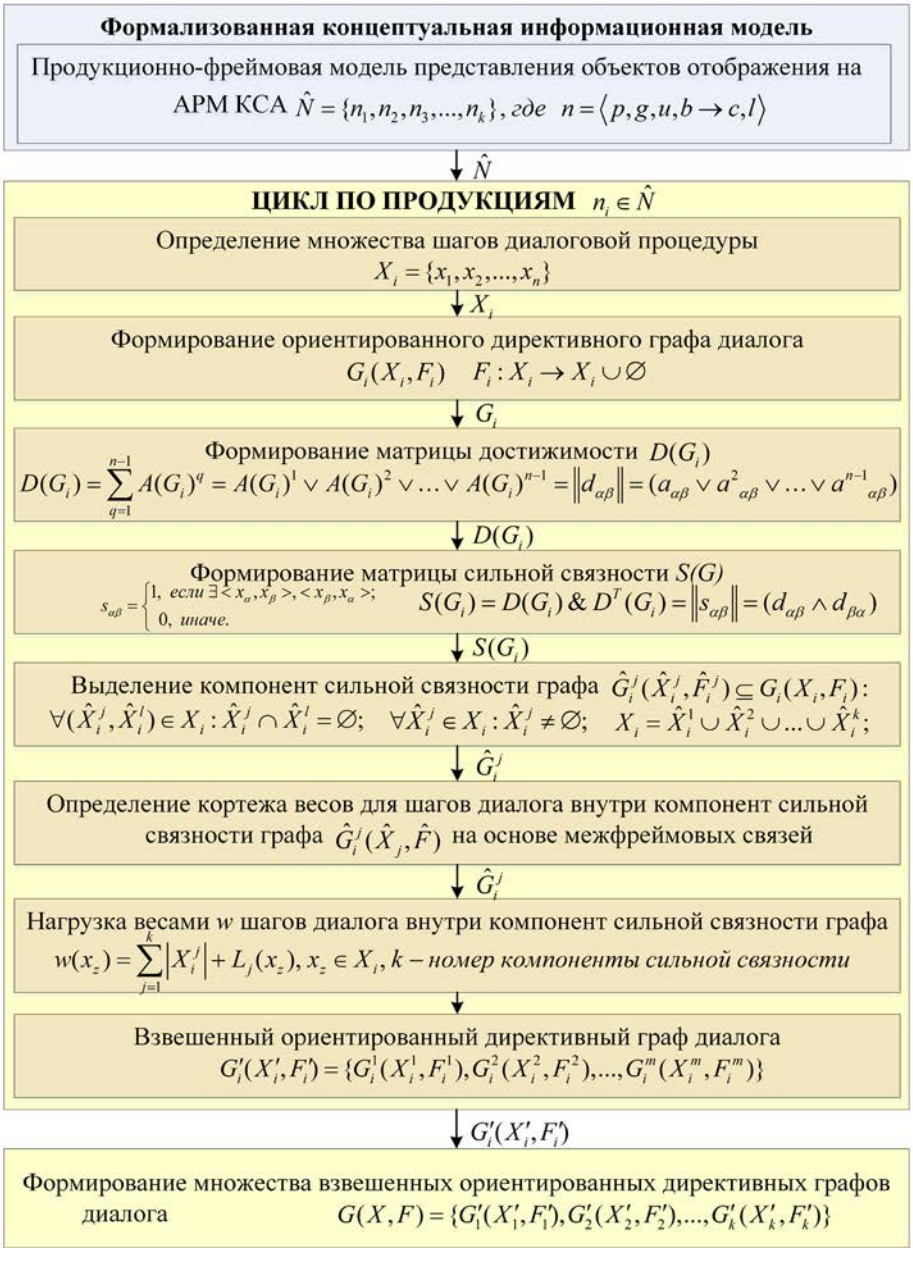


Рис. 4. Последовательность действий формирования множества взвешенных ориентированных директивных графов диалога

Формирование ориентированного графа диалога $G_i(X_i, F_i)$ требует последовательного осуществления двух процедур:

– выделение конечного множества шагов диалога $X_i \in X_\infty$;

– задание функции отображения F: $X \to X$ между шагами диалога.

Принимая во внимание сложность процесса диалогового взаимодействия между ЛБР и АРМ КСА выделение конечного множества шагов диалога $X_i \in X_\infty$ предлагается осуществить путем рассмотрения каждой полиадической задач управления отдельно. Исходной информацией для этого выступает продукционно-фреймовая модель (ПФМ) $\hat{N} = \left\langle \hat{P}; \hat{G}; \hat{U}; \hat{B}' \to \hat{C}'; \hat{L} \right\rangle$ представления объектов отображения на АРМ КСА. Антецедент ядра $b_i' \in \hat{B}'$ каждой продукции $\hat{n}_i \in \hat{N}, i = \overline{1,k}$ из состава ПФМ представляется в виде правил алгебры логики описывающих достаточность и взаимосвязь условий решения *i*-ой полиадической задачи управления. Таким образом, справедливо определить множество шагов диалога $X_i = \{x_1, x_2, \ldots, x_n\}$ для каждой отдельной *i*-ой полиадической задачи управления путем сопоставления шагов диалога с соответствующими им элементами антецедента ядра продукции $b_i' = \{\sigma^F_{in(1)}, \sigma^F_{in(2)}, ..., \sigma^F_{in(n)}\}$.

Выполнение процедуры определения функции отображения F_i между шагами диалога на множестве $X_i = \{x_1, x_2, \ldots, x_n\}$ производится путем анализа множества нормативных документов *W* на КСА. Содержащиеся в *W* алгоритмы решения полиадических задач управления, а также последовательность кадров меню предоставляемых ИМО задают связи между шагами диалога в виде ориентированных ребер $u_i \in U$.

Задачей следующего этапа является формирование приоритета порядка ввода данных. Отметим, что ЛБР при взаимодействии с АРМ КСА на естественно-подобном языке хоть имеет возможность выбора наиболее удобной для него точки входа в диалог, а также перехода между шагами диалога, условия решения задач управления накладывают на него ряд ограничений. Так, существуют задачи управления, в которых после ввода группы данных ЛБР получив промежуточный результат, анализирует его, продолжает ввод. Описанное обстоятельство приводит к возникновению таких шагов диалога x_i, для прохождения которых необходимо сначала пройти шаг диалога x_{i-1}. Следовательно структура графа диалога на естественно-подобном языке представляется в виде ориентированного слабо-связанного графа, т.е. выполняется условие что между двумя шагами диалога x_i, x_j может не оказаться соединяющих их ребер $u_k \in U$, но между ними обязательно должен существовать по крайней мере один соединяющий их маршрут. Данное обстоятельство приводит к необходимости разделения графа диалога на соответствующие компоненты сильной связности. С этой целью на множестве шагов диалога X_i вводится бинарное отношение эквивалентности «~» обладающее свойствами: рефлексивности $\forall x_i \in X : x_i \sim x_i$, симметричности $\forall x_i, x_j \in X : x_i \sim x_j \Rightarrow x_j \sim x_i$ и транзитивности $\forall x_i, x_j, x_z \in X : (x_i \sim x_j \wedge x_j \sim x_i) \wedge (x_j \sim x_z \wedge x_z \sim x_j) \Rightarrow x_i \sim x_z \wedge x_z \sim x_i$.

Данное отношение эквивалентности «~» порождает разбиение этого множества на классы эквивалентности $X_i^j \subseteq X_i$ или компоненты сильной связности графа диалога $\hat{G}_i^j$ удовлетворяющие следующим условиям:

– каждое из подмножеств $X_i^j \neq \varnothing$;

– два различных подмножества X_i^j и X_i^l, где $j \neq l$, не имеют общих элементов $X_i^j \neq X_j^l \to X_i^j \cap X_i^l = \varnothing$;

– объединение всех классов эквивалентности множества X_i равно этому множеству $\bigcup_{j=1}^{k} X_i^j = X_i$, где k — количество классов эквивалентности.

Учитывая описанные выше условия отметим, что компонентой сильной связности графа диалога $G_i(X_i, F_i)$ называется его подграф $\hat{G}_i^j$, не являющийся собственным подграфом другого связного подграфа $\hat{G}_i^j \not\subset \hat{G}_i^l$графа G_i.

Для нахождения компонент сильной связности, на графе диалога необходимо определить матрицу достижимости $D(G_i)$ и матрицу сильной связности $S(G_i)$.

Матрица достижимости $D(G_i)$ — это бинарная матрица замыкания по транзитивности отображения F_i, в которой содержится информация о существовании путей между шагами диалога X_i. Такая матрица формируется по следующему правилу:

$$d_{ij} = \begin{cases} 1, & \textit{если } \exists < x_i, x_j >; \\ 0, & \textit{иначе.} \end{cases}$$

где $< x_i, x_j >$ — путь из *i*-го шага диалога в *j*-й.

При построение такой матрицы необходимо учесть все пути длиной от 1 до $n-1$, где n — количество шагов диалога в графе. Длиной пути при этом называется число рёбер, используемых в пути. Заметим, что матрица смежности $A(G_i)$ дает информацию о всех путях длины 1, а для поиска путей длины 2 необходимо найти её композицию саму с собой:

$$A(G_i) \circ A(G_i) = \{< x_\alpha, x_\chi >: \exists x_\beta \in X_i :< x_\alpha, x_\beta >, < x_\beta, x_\chi > \in F\},$$

т.е.: $$A(G_i)^2 = \left\| a_{\alpha\beta}{}^2 \right\| = (\sum_k a_{\alpha k} a_{k\beta}) =$$

$$= ((a_{\alpha 1} \wedge a_{1\beta}) \vee (a_{\alpha 2} \wedge a_{2\beta}) \vee \ldots \vee (a_{\alpha n} \wedge a_{n\beta}))$$

Следуя, указанной выше логике после нахождения матриц $A(G_i)^k$ композиций $\underbrace{A(G_i) \circ \ldots \circ A(G_i)}_{k}$ для всех k, $1 \le k \le n-1$ будет получена информация о всех путях длины от 1 до n-1. При применении операции дизъюнкции на полученном множестве композиций формируется матрица достижимости $D(G_i)$ по следующему правилу:

$$D(G_i) = \sum_{q=1}^{n-1} A(G_i)^q = A(G_i)^1 \vee A(G_i)^2 \vee \ldots \vee A(G_i)^{n-1} =$$
$$= \left\| d_{\alpha\beta} \right\| = (a_{\alpha\beta} \vee a^2{}_{\alpha\beta} \vee \ldots \vee a^{n-1}{}_{\alpha\beta})$$

Матрица сильной связности $S(G_i)$ — это симметричная бинарная матрица, содержащая информацию о всех сильно связанных вершинах в графе диалога, заполняемая по правилу [6]:

$$s_{\alpha\beta} = \begin{cases} 1, & \textit{если } \exists < x_\alpha, x_\beta >, < x_\beta, x_\alpha >; \\ 0, & \textit{иначе.} \end{cases}$$

Построена такая матрица может быть из матрицы достижимости по формуле:

$$S(G_i) = D(G_i) \,\&\, D^T(G_i) = \left\| s_{\alpha\beta} \right\| = (d_{\alpha\beta} \wedge d_{\beta\alpha})$$

Дальнейшие действия по выделению компонент сильной связности основаны на анализе матрицы сильной связности $S(G_i)$. В данной матрице необходимо определить шаги диалога, которым соответствуют единицы в первой строке. Полученное множество $\hat{X}_i^{\,j}$ — это множество шагов диалога j-ой компоненты сильной связности $\hat{G}_i^{\,j}(\hat{X}_i^{\,j}, \hat{F}_i^{\,j})$. Удалив из матрицы сильной связности строки и столбцы, содержащие шаги диалога j-ой компоненты сильной связности необходимо повторить описанные действия до тех пор, пока не будет получена пустая матрица ∅, не имеющая ни столбцов, ни строк.

Описанные выше действия представлены в виде алгоритма рис. 5.

На первом этапе работы алгоритма определяются две вспомогательные переменные: p — для хранения количества компонент сильной связности которая на первом шаге инициализируется значением 0 и копию исходной матрицы сильной связности B. Далее проверяется условие что копия исходной матрицы B не является пустым множеством ∅. В случаи когда данное условие принимает значение «истинна», количество компонент сильной связности p увеличивается на единицу, а к множеству $\hat{X}_i^{\,p}$ добавляются шаги диалога которым соответствует единица в первой строке матрицы B. Матрица смежности для p-ой компоненты сильной связности $A_p(G_i)$ формируется путем выполнения двух вложенных циклов по всем строкам и столбцам матрицы B. В данном цикле проверяется условие существования ребер соединяющих шаги диалога в исходной матрице смежности $A(G_i)$. Если ребро существует в матрице $A(G_i)$, то делается вывод что оно существует и в его подматрице $A_p(G_i)$. Удалив из матрицы B строки и столбцы, соответствующие шагам диалога множества $\hat{X}_i^{\,p}$ возвращаемся

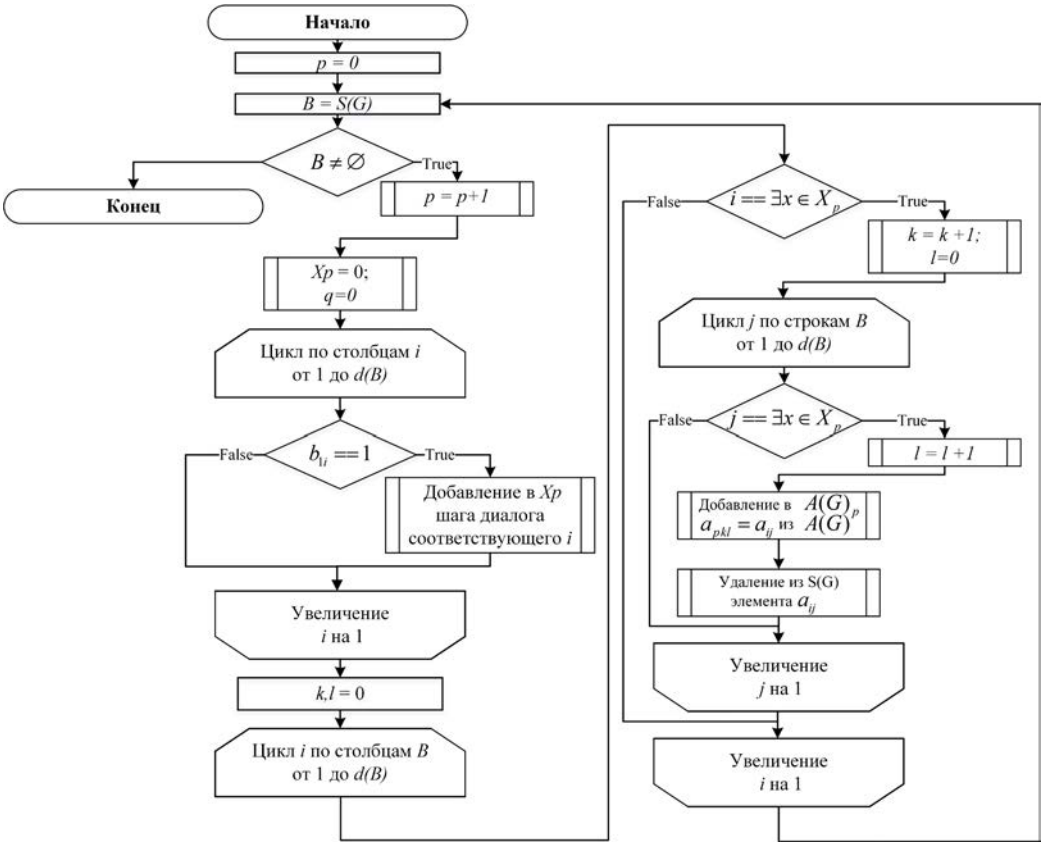


Рис. 5. Алгоритм выделения компонент сильной связности

к проверке первого условия: $B \neq \varnothing$ до тех пор пока оно не станет ложным. Когда данное условие становится ложным работа алгоритма заканчивается.

В результате выполнения данного алгоритма формируется:

– p — число компонент сильной связности;

– $\hat{X}_i^j$, $j = 1,2,\ldots,p$ — множество шагов диалога *j-той* компоненты сильной связности $\hat{G}_i(X_i, F) \subseteq G(X, F)$;

– $A_j(G_i), j = 1,2,\ldots,p$ — множество матриц смежности *j*-той компоненты сильной связности;

На следующем этапе необходимо определить приоритет шагов диалога внутри компонент сильной связности $\hat{G}_i^j$, $j = \overline{1,p}$. Для этого необходимо установить в какой взаимосвязи между собой находятся шаги диалога. К таким связям в частности возможно отнести отношения: «часть-целое», «общее — частное», «причина-следствие» и т.д. Заметим, что учет таких отношений возможно получить, проведя анализ межфреймовых связей используемой ранее для описания предметной области фреймовой модели. Этот механизм заключается в том, что некоторые слоты фрейма в качестве своих значений могут иметь другие фреймы. Такие слоты называются слотами связи, а отношения, представленные ими,— отношениями связи. Наличие слотов связи позволяет строить из фреймов различные сетевые структуры (сети фреймов), узлами которых являются фреймы, а связями — отношения (рис. 6) [17–20]. Все отношения, заданные в предметной области (ПО) содержатся в описанной выше фреймовой модели (ФМ).

Расстановка приоритета внутри компонент сильной связности на основе иерархии определяемой межфреймовыми связями позволит конкретизировать каждым следующим шагом диалога введенные ранее данные. Однако, учитывая, что ФМ всей ПО представляется в виде большой сложно структурированной сети предлагается произвести операцию выделения только той ее части, которая присутствует в компоненте сильной связности. Результатом такого выделения является фрагмент фреймовой модели $\text{ФМ}_i \subseteq$ ФМ содержащий информацию только о шагах диалога $X_i^j \subseteq X_i$ *j*-ой компоненты сильной связности.

Фрагмент $\text{ФМ}_i \subseteq$ ФМ возможно представить в виде ориентированного графа $G_{\text{ФМ}}(Y, U)$, где Y — вершины графа (уникальные имена фрейма или слота) отражающие множество показателей ПО, а U — ребра, связи между вершинами. Тогда определение приоритета внутри компоненты сильной связности $\hat{G}_i^j \subseteq G_i$ сводится к сравнению шагов диалога из множества $\hat{X}_i^j$с элементами Y ФМ начиная с фрейма верхнего уровня и до нижнего.

Осуществления операции сравнения на элементах ФМ требует введения операций: $\eta(F)$ — получения значения имени фрейма и $v(F)$ — получения значения слота. Также в соответствии с алгоритмом определения приоритета шагов диалога на основе межфреймовых связей (рис. 7) задается множество L содержащее шаги диалога упорядоченных в соответствии с отношением частичного порядка R на основе иерархии ФМ. Иерархия фреймовой модели определяется на основе расстояния $d(y_i)$ — числа ребер составляющих кратчайший путь от вершины фрейма верхнего уровня до вершины y_i. Элементы фреймовой модели находятся на одном уровне, если у них одинаковое расстояние. Отношение $x_i R x_j$ над шагами диалога x_i, x_j

Имя фрейма: ртб

Имя слота	Значение	Тип
Номер		Integer
Дислокация позиции		Integer
Обеспечиваемые КП		Frame
…	…	…
РЛС на вооружении		Frame

Имя фрейма: РЛС

Имя слота	Значение	Тип
Название		String
Длина волны		Integer
Тип антены		String
…	…	…
Сопровождаемые ВО		Frame

Имя фрейма: ВО

Имя слота	Значение	Тип
Номер		Integer
Тип		String
Скорость		Float
…	…	…
ЭПР		Float

Рис. 6. Фрагмент ИМ РМ КСА на основе фреймовой модели

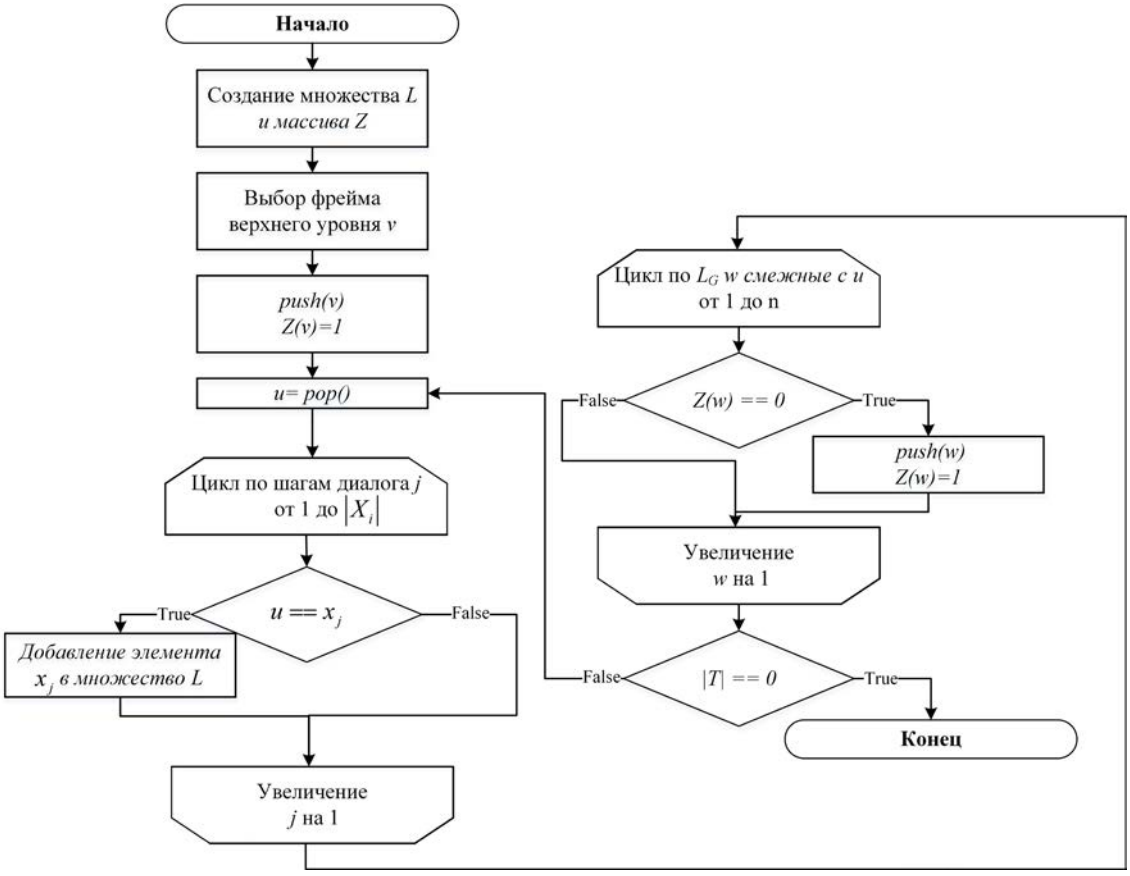


Рис. 7. Алгоритм определения приоритета шагов диалога на основе межфреймовых связей

говорит о том что шаг диалога x_i находится выше или на одном уровне иерархии с шагом диалога x_j.

Обход ФМ предлагается осуществить на основе поиска в ширину (breadth-first search, BFS). При поиске в ширину вершины обходятся по уровням, где посещается каждая вершина на определенном уровне прежде чем перейти на следующий. Поиск в ширину требует определения следующих структур данных:

Очередь T — является вспомогательным буфером. В нее временно помещаются обойденные вершины (это необходимо для обхода смежных вершин). В структуре данных типа очередь первый помещенный в нее элемент также извлекается первым (*first-in, first-out* — FIFO). Для очереди T определены следующие операции: *push*() — операция вставки нового элемента, *pop*() — операция удаления нового элемента, $|T|$ — операция получения количества элементов в очереди.

Массив Z — содержащий данные о том, была ли отмечена (пройдена) вершина. Длина Z равна количеству вершин. Каждый элемент массива соответствует одной вершине графа, полученной из ФМ и может принимать два значения:

1 — вершина отмечена (пройдена);

0 — вершина не отмечена.

Рассмотрим, работу алгоритма поэтапно:

1. создание пустого множества L_i и массива Z заполненного нулями. До начала обхода все вершины являются неотмеченными;

2. выбор вершины верхнего уровня v, с которой начинается обход.

3. вершина v добавляется в очередь T и отмечается в массиве Z как пройденная ($Z(v) = 1$);

4. из очереди T извлекается вершина u.

5. проведение в цикле сравнения элементов шагов диалога из множества $\hat{X}_i^j$. с вершиной u. В случае если результат сравнения «истина» — добавление в множество L_i элемента $x_j \in \hat{X}_i^j$.

6. по списку смежности графа построенного по ФМ L_G выбор вершин w смежных с v.

7. Если смежные с v вершины не были раннее отмечены (то есть, если $Z(w) = 0$), то они заносятся в очередь T и отмечаются как пройденные $Z(w) = 1$.

8. Если в очереди T находятся какие-либо вершины, то осуществляется переход к п. 4. Когда очередь T окажется пустой работа алгоритма завершена.

Полученное таким образом множество L определяет порядок шагов диалога внутри компоненты сильной связности.

Проведенные операции выделения компонент сильной связности и расстановка приоритета внутри них позволяют произвести нагрузку весами *w* шагов диалога $x_z \in \hat{X}_i^j$ по следующему правилу:

$$w(x_z) = \sum_{j=1}^{k} \left| X_i^j \right| + L_j(x_z),\ x_z \in X_i,$$

где *k* — номер компоненты сильной связности,

$L_j(x_z)$ — функция возвращающая положение элемента x_z в упорядоченном множестве L_j определенном для компоненты сильной связности $X_i^j \in X_i$.

Применение описанной выше последовательности действий для всех полиадических задач управления позволяет сформировать полное множество взвешенных ориентированных директивных графов диалога $G_i'(X_i', F_i') = \{G_i^1(X_i^1, F_i^1), G_i^2(X_i^2, F_i^2), ..., G_i^m(X_i^m, F_i^m)\}$, где *m* — количество полиадических задач управления.

Следующий этап работы способа позволяет учесть изменения, вносимые в структуру взвешенного ориентированного директивного графа диалога в зависимости от поступившего запроса на естественно-подобном языке. Последовательность действий, позволяющих учесть данные изменения и сформировать адаптивную структуру диалога представлена на рис. 8.

При получение запроса ЛБР З = ⟨К, У⟩происходит его предикатно-предметная интерпретация. В структуре запроса выделяются составляющие: К — команда, определяющая какую полиадическую задачу управления намерен выполнить ЛБР и У — множество условий содержащих данные необходимых для её решения.

СтруктурнокомандаЛБР $K(\alpha_1, \alpha_2) = \varphi(P_{K_1}(\alpha_1), P_{K_2}(\alpha_2))$ представляется в виде функции φ зависящей от двух командных предикатов $P_{K_1}(\alpha_1)$ и $P_{K_2}(\alpha_2)$. В командном предикате $P_{K_1}(\alpha_1)$ объектная переменная α_1 представляет собой действие на которое направлена команда («рассчитать», «показать», «вызвать» и т.д.), а объектная переменная α_2 из командного предиката $P_{K_2}(\alpha_2)$ полное или одно из сокращённых названий полиадической задачи управления заданных в виде списка синонимов. После получении команды *K* производится ее интерпретация, и проверка на соответствие условиям применимости ядра продукции $u_i \in \hat{U}$ из состава ПФМ. Такая проверка позволяет определить какую полиадическую задачу управления намерен решить ЛБР и выделить соответствующий ей взвешенный ориентированный директивный граф диалога $G_i'(X_i', F_i')$. В том случае когда команда не соответствует ни одному условию применимости ядра продукций, генерируется сигнал об отсутствии требуемой команды *K*.

Множество условий естественно-языкового запроса ЛБР представляет из себя *n*-местный предикат $P_Y(y_1, y_2, ..., y_n)$, где в качестве множества объектных переменных $Y = \{y_1, y_2, ..., y_n\}$ выступают вводимые ЛБР данные. Каждая объектная переменная $y_i \in Y$ представляется высказыванием на естественно-подобном языке вида: y_i = ⟨"*понятие*", "*значение*"⟩, например «высота 100 м.», «скорость 100 м/с», «112 рлр» и т.д.

Отметим, что в процессе взаимодействия на естественно-подобном языке возможны случаи, когда ЛБР введет некорректные или, вовсе не участвующие в решение данной полиадической задачи управления данные (объектные

Рис. 8. Последовательность действий по формированию адаптивной структуры диалога

переменные). Устранение ошибок такого рода требует проведения операции по верификации данных (объектных переменных) поступающих в условии запроса на естественно-подобном языке путем выполнения двух процедур:

1. поиска взаимного соответствия между объектными переменными $y_i \in Y$ *n*-местного предиката $P_{\text{У}}(y_1, y_2, ..., y_n)$ и шагами диалога взвешенного ориентированного директивного графа диалога $X_i' = \{x_1, x_2, ..., x_n\}$;

2. проверки множества условий по области допустимых значений.

Выполнение данных процедур для каждой объектной переменной $y_i \in Y$ требует введения операций по выделению ее составляющих: «имени понятия» $\eta(y_i)$ и «значения понятия» $v(y_i)$. Отметим, что под понятием *P* понимается класс сущностей, объединяемых на основе общности структур. Любое понятие характеризуется заданной для него областью допустимых значений и уникальным именем. Имя понятия выполняет роль уникального идентификатора, определяя понятие среди остальных и может быть выражено на естественно-подобном языке в виде слова или словосочетания.

Для осуществления первой процедуры предлагается произвести поиск взаимного соответствия между данными поступившими в условии запроса и шагами диалога на основе сравнения имен понятий $\eta(y_i)$ и названий шагов диалога директивного графа диалога $x_j \in X_i'$ Если результат операции сравнения принимает значение «истина», тогда данное понятие ассоциируется с шагом диалога. В противном случае принимается решение, что данное понятие не участвует в решение данной полиадической задачи управления. В результате работы данной процедуры выделяется множество входных условий $\text{У}_{in} = y_i \in \text{У} \,|\, y_i \subseteq X$ однозначно соотнесенное с шагами диалога *i*-го директивного графа диалога.

Задачей следующей процедуры является проверка множества входных условий У_{in} на соответствие его допустимого значения. Отметим, что с каждым условием $y_i \in \text{У}_{in}$ соотносится один из ранее определенных элементов ФМ с заданной ему областью допустимых значений. Таким образом, для выполнения данной процедуры необходимо проверить удовлетворяют ли поступившие значения условий, множеству ограничений, заданному для соответствующих им значениям слотов фрейма $\hat{\sigma}_{\text{У}}^F = \{\sigma_1^F, \sigma_2^F, ..., \sigma_l^F\}$ в виде набора правил или предикатов. С этой целью определяется функция $\psi(\sigma_j^F)$, возвращающая значение «истина» если значение поступившего условия удовлетворяет ограничениям значений слотов заданных в фреймовой модели, и «ложно» в противном случае. Примените данной функцию для каждого входного условия позволяет сформировать множество верифицированных условий запроса ЛБР $\hat{\text{У}}_{in}$ по следующему правилу:

$$\hat{\text{У}}_{in} = \{y_i \in \text{У}_{in} \mid y_i \subset \psi(\sigma_j^F)\}$$

На следующем этапе построения адаптивного сценария диалоговой процедуры необходимо представить условия запроса ЛБР в виде пустого графа или нуль-графа $G_i^{\varnothing}(X_i^{\hat{\text{У}}_{in}}, F)$. Пустой граф — это регулярный граф степени 0, содержавший вершины $X_i^{\hat{\text{У}}_{in}}$ образованные по правилу $X_i^{\hat{\text{У}}_{in}} = \{x_j \in X_i' \mid x_j \sim y_l\}$, где $y_l \in \hat{\text{У}}_{in}$, не имеющие связей между собой $F = \varnothing$.

Формирование директивного графа диалога адаптивного запросу ЛБР предлагается осуществить путем введения операцию вычитания между директивным графом диалога и пустым графом $G_i'(X_i', F_i') / G_i^{\varnothing}(X_i^{\hat{\text{У}}_{in}}, F)$. В результате проведения данной операции формируется множество результирующих шагов диалога $\overline{X} = X_i' \setminus X_i^{\hat{\text{У}}_{in}}$, и результирующая функция отображения $\overline{F}$ содержащая те и только те переходы между шагами диалога исходного взвешенного ориентированного директивного графа диалога G_i', которые не инцидентны $X_i^{\hat{\text{У}}_{in}}$.

Заключение

Проведенная последовательность действий позволяет определить адаптивный сценарий диалога путем расстановки множества результирующих шагов диалога по правилу наименьшего значения веса *w*. Сформированный таким образом адаптивный сценарий диалога содержит необходимый порядок запросов со стороны АРМ КСА к ЛБР с целью получения данных, недостающих для решения требуемой полиадической задачи управления. В сценарии построенном по такому принципу каждый последующий шаг диалога уточняет предыдущий и является основой построения диалоговой системы взаимодействия между ЛБР и АРМ КСА.

Литература

1. *Фененко А.В.* Концепция «быстрого глобального удара» в контексте развития военной стратегии США // Вестник Московского университета. Серия 25. Международные отношения и мировая политика. 2016. № 4. С. 18–50.

2. *Попов И.М. Хамзатов М.М.* Война будущего: концептуальные основы и практические выводы. Очерки стратегической мысли. М.: Кучково поле, 2016. 832 с.

3. *Макаров К.В., Ченцов А.Е.* Крылатые ракеты противника — фактор изменения в соотношении сил воюющих сторон // Военная мысль. 2017. № 10. С. 52–57.

4. *Бориско С.Н., Горемыкин С.А.* Анализ состояния воздушно-космических сил России. Перспективы развития // Военная мысль. 2019. № 1. С. 25–37.

5. *Фисенко Н.А.* Анализ влияния тенденций развития средств воздушного нападения противника, форм и способов их боевого применения на живучесть базирования авиации // Воздушно-космические силы. Теория и практика. 2017. № 3. С. 32–38.

6. *С.В. Суровикин, Ю.В. Кулешов.* Особенности организации управления межвидовой группировкой войск (сил) в интересах комплексной борьбы с противником // Военная мысль.2017. № 8. С. 5–18.

7. *Морозов П.А., Круталевич Ю.А., Аношин Р.И., Зюзина А.Д.* Одно из направлений сокращения времени принятия решения оператором автоматизированного рабочего места комплекса средств

автоматизации на основе формализованной концептуальной модели воздушной обстановки // Международная научно-практическая конференция «Путь в науку 2018» Ярославль, 2018. С 223–235.

8. *Посевкин Р.В*. Применение семантической модели базы данных при реализации естественно-языкового пользовательского интерфейса // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 2. С. 262–267.

9. *Морозов П.А., Зюзина А.В., Круталевич Ю.А., Аношин Р.И,* Способ сокращения работного времени комплекса средств автоматизации на основе применения запросов на естественно-подобном языке // Радиотехника. 2020. № 3 С. 5–15.

10. Патент РФ 2737598. Способ формирования оперативной информации на основе формализованной концептуальной модели предметной области / Морозов П. А., Аношин Р. И., Круталевич Ю. А., Зюзина А. Д. Заявл. 04.02.2020. Опубл. 1.12.2020. Бюл.№ 11. 3 с.

11. *Посевкин Р.В., Бессмертный И.А*. Естественно-языковой пользовательский интерфейс диалоговой системы // Программные продукты и системы. 2016. № 3. С. 5–9.

12. *Барышникова Н.Ю*. Обработка запросов на естественно-подобном языке на основе семантических сетей и шаблонов // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. 2016. № 4. С. 36–45.

13. *Попов Э.В., Ляшенко Е.Н*. Онтологическая модель представления знаний в интеллектуальной системе управления процессами ликвидации последствий чрезвычайных ситуаций природного характера // Вестник Херсонского национального технического университета. 2017. № 2 (61) С. 218–227.

14. *Попов Э.В*. Общение с компьютером на естественном языке. М.: ЛЕНАНД,2021. 360 с.

15. *Говоритель В.В*. Развитие средств информационного обеспечения деятельности оператора автоматизированных и информационных систем военного назначения // Научно-методический сборник Международной военно-научной конференции. Тверь, 2017. С 133–141.

16. *Морозов П.А*. Способ формализации концептуальной информационной модели рабочего места комплекса средств автоматизации военного назначения // Радиотехника. 2020. № 3. С. 16–27.

17. *Мисевич П.В., Ермилов А.Э*. Инструментальная система построения ситуационного описания в форме иерархической сети фреймов // Материалы XVI Всероссийской научной конференции «нейрокомпьютеры и их применение» (Москва, 13 марта 2018 г.). Москва, 2018. С. 37.

18. *Шеланков О.Е., Мясин П.Ю., Андосов А.И., Кривцов П.А*. Особенности применения логического и алгебраического подходов к формированию сценариев на основе сетей событийных фреймов // Радиопромышленность. 2017. № 1. С. 119–123.

19. *Саркисян К.Р.* Модель знаний системы поддержки принятия решений для оценки наукоемких проектов // Материалы XXI–XXII Международной научно-практической конференции. Новосибирск, 2018. С12–16.

20. *Юрина Н.Н., Волошина О.В., Тошкина А.А.* Искусственный интеллект: основные задачи и методы // Материалы IV Всероссийской научно-практической конференции (с международным участием) «Информационные технолоогии в Экономике и управлении» (Махачкала, 11–12 ноября 2020 г.). Махачкала, 2020. С142–146.

METHODOLOGY OF FORMATION OF ADAPTIVE DIALOGUE SCENARIO WHEN SOLVING AUTOMATED CONTROL TASKS AT THE WORKPLACE OF A COMPLEX OF AUTOMATION MEANS FOR MILITARY PURPOSE

ALEXEY V. ZYUZIN

Yaroslavl, Russia, aleksey.zyuzin@mail.ru

VICTOR A. KURCHIDIS

Yaroslavl, Russia, idahmer2@yandex.ru

PAVEL A. MOROZOV

Yaroslavl, Russia, mpa24@mail.ru

ROMAN I. ANOSHIN

Yaroslavl, Russia, roman88an@gmail.com

KEYWORDS: management efficiency; management tasks; natural-language interaction; production-frame model; dialogue step; dialogue graph.

ABSTRACT

The analysis shows that in the period of immediate threat of aggression and, especially in wartime, there is a need to improve the effectiveness of the management of troops, by reducing the working time of the combat calculation of the control body when solving polyadic management tasks. One of the most preferred ways to reduce the working time of the combat crew of the control body is to use a dialog mode of interaction between the persons of the combat crew and the automated workplace of the automation complex based on the use of queries in a natural-like language. One of the elements necessary for the organization of such interaction, which allows you to take into account the sequence of steps of the dialogue, depending on the needs of the combat crew, is an adaptive dialogue scenario. The dialog structure is represented as a set of weighted directed dialog graphs. This formalization allows you to take into account the sequence of data input when solving management problems by highlighting the components of strong connectivity and deter-

mining the order of dialogue steps within them based on the relationships of inter-frame relationships. In order to take into account changes made to the structure of the weighted oriented Directive graph of the dialog, depending on the received request in a natural-like language, the structural components of the command and a set of conditions are highlighted in the request of the combat crew members. The set of conditions after predicate-subject interpretation and checking for correctness of the value is represented as an empty graph. The subtraction operation between the weighted oriented Directive graph of the dialog and the empty graph allows you to generate a set of resulting dialog steps and determine the transition function between them. Placing the dialog steps in ascending order of priority, determined on the basis of a weighted oriented Directive graph, forms an adaptive dialog scenario.

REFERENCES

1. Fenenko A.V. The concept of a "rapid global strike" in the context of the development of the US military strategy. *Vestnik of Moscow University. Series 25. International relations and world politics*. 2016. No. 4. Pp. 18–50. (In Rus)
2. Popov I.M., Khamzatov M.M. *Vojna buduschego: konceptual'nye osnovy i prakticheskie vyvody. Ocherki strategicheskoj mysli* [The War of the future: conceptual foundations and practical conclusions. Essays of strategic thought]. Moscow: Kuchkovo field, 2016. 832 p. (In Rus)
3. Makarov K.V., Chentsov A.E. Enemy cruise missiles-a factor of change in the ratio of forces of the warring parties. *Military thought*. 2017. No. 10. Pp. 52–57. (In Rus)
4. Borisko S.N., Goremykin S.A. Analysis of the state of the Russian aerospace forces. Development prospects. *Military thought*. 2019. No. 1. Pp. 25–37. (In Rus)
5. Fisenko N.A. Analysis of the influence of trends in the development of enemy air attack means, forms and methods of their combat use on the survivability of aviation bases. *Aerospace forces. Theory and practice*. 2017. No. 3. Pp. 32–38. (In Rus)
6. Surovikin S.V., Kuleshov Yu.V. Features of the organization of management of an interspecific grouping of troops (forces) in the interests of a comprehensive fight against the enemy. *Military thought*. 2017. No. 8. Pp. 5–18. (In Rus)
7. Morozov P.A., Krutalevich Yu. A., Anoshin R.I., Zyuzina A.D. One of the directions of reducing the time of decision-making by the operator of an automated workplace of a complex of automation tools based on a formalized conceptual model of the air situation. *International scientific and practical conference "The way to Science 2018"*. Yaroslavl, 2018. Pp. 223–235. (In Rus)
8. Posevkin R.V. Application of the semantic model of the database in the implementation of the natural language user interface. *Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics*. 2018. Vol. 18. No. 2. Pp. 262–267. (In Rus)
9. Morozov P.A., Zyuzina A.V., Krutalevich Yu. A., Anoshin R.I., A method for reducing the working time of a complex of automation tools based on the use of queries in a natural-like language. *Radiotehnika*. 2020. No. 3. Pp. 5–15. (In Rus)
10. Patent RF 2737598. Sposob formirovaniya operativnoj informacii na osnove formalizovannoj konceptual'noj modeli predmetnoj oblasti [A method for forming operational information on the basis of a formalized conceptual model of the subject area]. Morozov P.A., Anoshin R.I., Krutalevich Yu. A., Zyuzina A.D. Application 04.02.2020. Publ. 1.12.2020. Byul. No. 11. 3 p. (In Rus)
11. Posevkin R.V., Bessmertny I.A. Natural-language user interface of the dialog system. *Programmnye produkty i sistemy*. 2016. No. 3. Pp. 5–9. (In Rus)
12. Baryshnikova N. Yu. Processing of requests in a natural-like language based on semantic networks and templates. *Vestnik of Astrakhan state technical university. Series: Management, Computer engineering and Computer Science*. 2016. No. 4. Pp. 36–45. (In Rus)
13. Popov E.V., Lyashenko E.N. Ontological model of knowledge representation in the intellectual management system of processes of elimination of consequences of emergency situations of natural character. *Bulletin of the Kherson National Technical University*. 2017. No. 2 (61). Pp. 218–227. (In Rus)
14. Popov E.V. *Obschenie s komp'yuterom na estestvennom yazyke* [Communication with a computer in a natural language]. Moscow: LENAND, 2021. 360 p. (In Rus)
15. Govoritel V.V. Development of information support tools for the operator of automated and information systems for military purposes. *Scientific and methodological collection of the International Military-Scientific Conference*. Tver, 2017. Pp. 133–141. (In Rus)
16. Morozov P.A. The method of formalization of the conceptual information model of the workplace of the complex of automation tools for military purposes. *Radiotehnika*. 2020. No. 3. Pp. 16–27. (In Rus)
17. Misevich P.V., Ermilov A.E. Tooling system build situational descriptions in the form of a hierarchical network of frames. *Proceedings of the XVI all-Russian scientific conference "Neurocomputers and their application", Moscow, March 13, 2018*. Moscow, 2018. P. 37. (In Rus)
18. Shelankov O.E., P.Y. Massine, Andosov I.A., Krivtsov A.P. features of the application of logical and algebraic approaches to the development of scenarios based on networks of event frames. *Radiopromyshlennost'* [Radio industry]. 2017. No. 1. Pp. 119–123. (In Rus)
19. Sarkisyan K.R. Model of knowledge of the decision support system for evaluating high-tech projects. *Proceedings of the XXI–XXII International Scientific and Practical Conference*. Novosibirsk, 2018. Pp. 12–16. (In Rus)
20. Yurina N.N., Voloshin, O. V., Toskin A.A. Artificial intelligence: basic problems and methods. *Proceedings of the IV all-Russian scientific-practical conference (with international participation) "Information tehnoloogia in Economics and management", Makhachkala, November 11–12, 2020*. Makhachkala, 2020. Pp. 142–146. (In Rus)

INFORMATION ABOUT AUTHOR:

Zyuzin A.V., PhD., full professor, Head of the Yaroslavl higher military school of air defense;
Kurchidis V.A., PhD., Full Professor, professor of the Yaroslavl higher military school of air defense;
Morozov P.A., PhD, Docent, Doctoral candidate of the Yaroslavl higher military school of air defense;
Anoshin R.A., Postgraduate of the Yaroslavl higher military school of air defense.

For citation: Zyuzin A.V., Kurchidis V.A., Morozov P.A., Anoshin R.A. Methodology of formation of adaptive dialogue scenario when solving automated control tasks at the workplace of a complex of automation means for military purpose. *H&ES Research*. 2021. Vol. 13. No. 3. Pp. 36–47. Doi: 10.36724/2409-5419-2021-13-3-36-47 (In Rus)

Doi: 10.36724/2409-5419-2021-13-3-48-59

МЕТОДИЧЕСКИЕ И ПРОГРАММНЫЕ СРЕДСТВА ВЫБОРА РЕШЕНИЙ ПО СОЗДАНИЮ (РАЗВИТИЮ) АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

ЛЯСКОВСКИЙ
Виктор Людвигович[1]

БРЕСЛЕР
Игорь Борисович[2]

АЛАШЕЕВ
Михаил Александрович[3]

АННОТАЦИЯ

Введение: к настоящему времени вопросы обоснования, оценки и выбора вариантов создания (развития) автоматизированных систем управления специального назначения недостаточно формализованы и не позволяют при выборе решений комплексно учитывать совокупность ряда значимых параметров: директивно заданные решения; классификационные признаки органов управления; функциональные процессы высшего приоритета; заданные предельно допустимые вероятностно-временные и временные характеристики выполнения функциональных процессов; требования к защите информации; конструктивные и надежностные требования; технологические возможности предприятий-исполнителей; допустимые временные и стоимостные параметры процесса создания системы; риски несвоевременной реализации решений по разработке, изготовлению средств автоматизации и оснащению ими органов управления. **Цель исследования:** разработка методических и программных средств выбора решений по созданию (развитию) автоматизированных систем управления специального назначения, обеспечивающих максимизацию эффективности выполнения функциональных процессов в системе с учетом заданных требований и ограничений. **Методы:** предложены методические средства, включающие формализацию структуры автоматизированных систем управления специального назначения, постановку задачи выбора решений по их созданию (развитию), а также алгоритм решения поставленной задачи, основанный на применении «жадных» методов дискретной оптимизации. **Результаты:** разработанные методические средства реализованы в виде специализированных программных средств, являющихся основой программного комплекса поддержки принятия решений, позволяющего в автоматизированном режиме находить решение поставленной задачи, а именно формировать рациональный вариант решений по разработке, изготовлению и продлению эксплуатации комплексов средств автоматизации для органов управления из состава автоматизированных систем управления специального назначения. **Практическая значимость:** результаты исследования могут быть использованы при обосновании федеральных и ведомственных целевых программ по разработке и модернизации распределенных информационно-управляющих систем специального назначения. **Обсуждение:** использование разработанных методических и программных средств позволит повысить обоснованность и сократить трудоемкость процессов формирования решений по созданию (развитию) автоматизированных систем управления специального назначения.

КЛЮЧЕВЫЕ СЛОВА: автоматизированная система управления специального назначения; комплекс средств автоматизации; выбор решений по созданию и развитию автоматизированных систем управления; эффективность автоматизированной системы управления; программный комплекс поддержки принятия решений.

Сведения об авторах:
[1]д.т.н., профессор, главный научный сотрудник АО «Научно-исследовательский институт информационных технологий», г. Тверь, Россия, dop_big@mail.ru

[2]д.т.н, доцент, генеральный директор АО «Научно-исследовательский институт информационных технологий», г. Тверь, Россия, niiit@niiit.tver.ru

[3]к.т.н., специалист АО «Научно-исследовательский институт информационных технологий», г. Тверь, Россия, mihal81@mail.ru

Для цитирования: *Лясковский В.Л., Бреслер И.Б., Алашеев М.А.* Методические и программные средства выбора решений по созданию (развитию) автоматизированных систем управления // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13. № 3. С. 48–59. Doi: 10.36724/2409-5419-2021-13-3-48-59

Введение

Одним из основных путей повышения эффективности процессов обработки информации и управления в многоуровневых иерархических системах специального назначения (к таким системам относятся, например, силовые министерства и ведомства, агентства, различные ведомственные формирования) является комплексная автоматизация процессов обработки информации и управления, реализуемая в процессе создания (развития) соответствующих автоматизированных систем управления специального назначения (АСУ СН).

АСУ СН — это распределенные многоуровневые автоматизированные системы обработки информации и управления, состоящие из множества функциональных подсистем (ФПс), каждая из которых реализует ряд взаимоувязанных функциональных процессов (ФП). Функциональные процессы, в свою очередь, реализуются посредством выполнения взаимосвязанных функциональных задач (ФЗ), решаемых на различных уровнях управления.

Под созданием АСУ СН понимается комплекс работ, направленных на создание новой автоматизированной системы, не существовавшей ранее.

Под развитием АСУ СН понимается комплекс работ, направленных на реализацию в существующей автоматизированной системе новых ФЗ, ФП и ФПс.

Формализация структуры АСУ СН

Типовая структурная схема АСУ СН приведена на рис. 1 и включает в свой состав подсистему обработки информации, подсистему передачи информации, а также подсистему внешних объектов [1]. При этом подсистема обработки информации АСУ СН состоит из органов и объектов управления (ОУ), которые, как правило, включают в свой состав центр обработки информации и управления (ЦОИУ), а также пункты обработки информации и управления (ПОИУ) различных иерархических уровней. Центр и пункты обработки информации являются объектами информатизации и могут быть реализованы в стационарном, перебазируемом и подвижном (мобильном) исполнении. Основными подсистемами центра и пунктов обработки информации выступают подсистема автоматизации деятельности должностных лиц, которая реализуется на основе соответствующих комплексов средств автоматизации (КСА), а также обеспечивающие подсистемы: энергоснабжения, обеспечения жизнедеятельности должностных лиц и др.

КСА обеспечивают автоматизированное выполнение ФЗ, являющихся составными частями ФП, которые, в свою очередь, входят в состав соответствующих ФПс.

Подсистема передачи информации состоит из трактов передачи данных и обеспечивает информационное взаимодействие всех элементов АСУ СН. Как правило, подсистема передачи информации включает собственные и арендуемые линии и узлы связи.

Подсистема внешних объектов включает в свой состав источники и потребители информации.

Постановка задачи выбора решений по созданию (развитию) АСУ СН

Создание АСУ СН предполагает проектирование (модернизацию) КСА для различных иерархических уровней системы (именно в них реализуется автоматизация соответствующих ФПс, ФП и ФЗ), изготовление серийных образцов КСА, а также оснащение ими ОУ из состава системы.

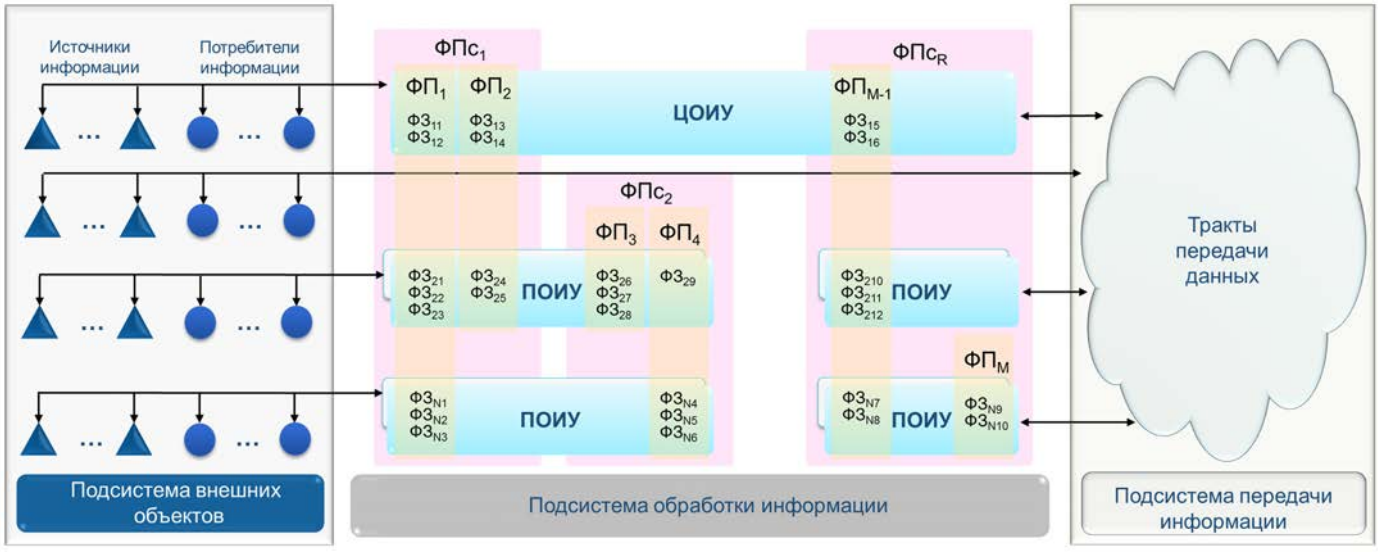


Рис. 1. Типовая структурная схема АСУ СН

При этом, исходя из существующего порядка выполнения работ по автоматизации ОУ, при обосновании рационального варианта по созданию (развитию) АСУ СН необходимо учитывать имеющиеся ограничения по выделяемым ассигнованиям на эксплуатацию существующих, производство серийных образцов и проектирование перспективных КСА.

Решения по созданию (развитию) АСУ СН подразделяются на три группы [1]:

– решения по разработке КСА — комплекс решений, формируемых на предпроектной стадии (в ходе выполнения научно-исследовательских работ) и стадии проектирования КСА (в ходе выполнения опытно-конструкторских работ), определяющих перечень, состав, структуру и характеристики КСА, а также состав организаций, участвующих в разработке КСА;

– решения по изготовлению КСА и оснащению ОУ — комплекс решений, определяющих последовательность, сроки и стоимость изготовления КСА и их поставки на ОУ, а также состав организаций, участвующих в изготовлении КСА и оснащении ОУ;

– решения по обеспечению эксплуатации и продлению ресурса эксплуатации КСА — комплекс решений, определяющих последовательность, сроки и стоимость продления эксплуатации КСА на ОУ, а также состав организаций, участвующих в продлении ресурса эксплуатации КСА.

Подобный вариант разделения позволяет последовательно охватить все основные стадии жизненного цикла КСА из состава АСУ СН. Предлагаемый подход к разделению системотехнических решений на группы соответствует модели жизненного цикла автоматизированных систем, принятому в ГОСТ 34-й серии.

Ряд теоретических исследований, связанных с вопросами выбора системотехнических, схемотехнических и организационных решений по созданию (развитию) автоматизированных систем управления, информационных систем организационного типа и оснащению ими соответствующих ОУ известны и описаны в литературе. Так, например, в [1–8] рассмотрены некоторые подходы к оценке эффективности функционирования АСУ СН, их подсистем и элементов, а также ряд частных постановок задач и соответствующих методов (научно-методических подходов) по выбору ряда системотехнических, схемотехнических и организационных решений для различных этапов жизненного цикла указанного класса систем.

Тем не менее, на сегодняшний момент времени вопросы обоснования, оценки и выбора вариантов создания (развития) АСУ СН недостаточно формализованы и не позволяют при выборе решений комплексно учитывать следующую совокупность значимых параметров [1–4, 8–16]:

– директивно заданные решения (решения, задаваемые пользователем);

– классификационные признаки ОУ;

– функциональные процессы высшего приоритета (ФПв);

– заданные предельно допустимые вероятностно-временные и временные характеристики (ВВХ и ВХ) выполнения ФП;

– заданные требования к защите информации;

– конструктивные и надежностные требования;

– технологические возможности предприятий-исполнителей;

– допустимые временные и стоимостные параметры процесса создания (развития) АСУ СН;

– риски несвоевременной реализации решений по разработке, изготовлению КСА и оснащению ими ОУ.

Учет указанных параметров произведен путем следующей постановки задачи выбора.

Необходимо определить вариант решений по созданию (развитию) АСУ СН $X^*(u)$, $Y^*(u)$, $Z^*(u)$, обеспечивающий максимизацию эффективности выполнения ФП $E(X(u), Y(u), Z(u))$ при обязательном выборе директивно заданных решений $X'(u)$, $Y'(u)$, $Z'(u)$, обязательной реализации ФПв, заданных предельно допустимых ВВХ и ВХ выполнения ФП, при выполнении заданных требований к защите информации $\mathfrak{V}^{з.и}_{тр}$, конструктивным $\mathfrak{V}^{к}_{тр}$ и надежностным характеристикам КСА $\mathfrak{V}^{н}_{тр}$, при выполнении ограничений на технологические возможности предприятий-исполнителей $W_{доп}$, временные $T_{доп}$ и стоимостные $C_{доп}$ параметры процесса создания (развития) АСУ СН, а также на риски несвоевременной реализации решений по разработке КСА $R^{р}_{доп}$, изготовлению КСА и оснащению ими ОУ $R^{и}_{доп}$:

$$X^*(u), Y^*(u), Z^*(u) = \underset{X(u),Y(u),Z(u)}{\arg\max} \; E(X(u), Y(u), Z(u)), \quad (1)$$

при выполнении ограничений:

$X^*(u) \cap X'(u) = X'(u)$;
$Y^*(u) \cap Y'(u) = Y'(u)$;
$Z^*(u) \cap Z'(u) = Z'(u)$;
$\Omega(X(u), Y(u)) \cap \Omega_в = \Omega_в$;
$\Omega'_{р.в} \cup \Omega''_{р.в} = \Omega_{р.в}$;
$\Omega'_{р.в} \cap \Omega''_{р.в} = \varnothing$;
$\forall i,\ i \in \Omega'_{р.в}$: $P_i(t_i(X(u), Y(u), Z(u)) \le t^{тр}_i) \ge P^{тр}_i$;
$\forall i,\ i \in \Omega''_{р.в}$: $\tau_i(X(u), Y(u), Z(u)) \le \tau^{тр}_i$;
$\mathfrak{V}^{з.и}(X(u), Y(u), Z(u)) \cap \mathfrak{V}^{з.и}_{тр} = \mathfrak{V}^{з.и}_{тр}$;
$\mathfrak{V}^{к}(X(u), Y(u), Z(u)) \cap \mathfrak{V}^{к}_{тр} = \mathfrak{V}^{к}_{тр}$;
$\mathfrak{V}^{н}(X(u), Y(u), Z(u)) \cap \mathfrak{V}^{н}_{тр} = \mathfrak{V}^{н}_{тр}$;
$\forall j, j \in M$: $W_j(X(u), Y(u), Z(u)) \cap W^{доп}_j(u) = W_j(X(u), Y(u), Z(u))$;
$C(X(u), Y(u), Z(u)) \le C_{доп}(u)$;
$T(X(u), Y(u), Z(u)) \le T_{доп}(u)$;
$R(X(u)) \le R^{р}_{доп}$; $R(Y(u)) \le R^{и}_{доп}$;

где $X(u)$ — решения по разработке КСА;

$Y(u)$ — решения по изготовлению КСА и оснащению органов управления;

$Z(u)$ — решения по обеспечению эксплуатации и продлению ресурса КСА;

$u \in \{1, \ldots U\}$, U — количество плановых ЭП создания (развития) АСУ СН;

$X'(u)$ — множество директивно заданных решений по разработке КСА;

$Y'(u)$ — множество директивно заданных решений по изготовлению КСА и оснащению ОУ;

$Z'(u)$ — множество директивно заданных решений по продлению ресурса эксплуатации КСА;

Ω — множество реализованных ФП;

$\Omega_в$ — множество ФПв;

$\Omega_{р.в}$ — множество ФП реального времени;

$\Omega'_{р.в}$ — множество ФП реального времени, для которых предъявляются требования к ВВХ их реализации;

$\Omega''_{р.в}$ — множество ФП реального времени, для которых предъявляются требования к ВХ их реализации;

P_i — вероятность своевременного выполнения i-го ФП;

t_i — время выполнения i-го ФП;

$t_i^{тр}$ — требуемое (директивное) время выполнения i-го ФП;

$P_i^{тр}$ — требуемая вероятность своевременного выполнения i-го ФП;

τ_i — среднее время выполнения i-го ФП;

$\tau_i^{тр}$ — требуемое среднее время выполнения i-го ФП;

$\mathfrak{Ю}^{з.и}$ — множество реализуемых требований к защите информации;

$\mathfrak{Ю}^{з.и}_{тр}$ — множество заданных требований к защите информации;

$\mathfrak{Ю}^{к}$ — множество реализуемых требований к конструктивным характеристикам КСА;

$\mathfrak{Ю}^{к}_{тр}$ — множество заданных требований к конструктивным характеристикам КСА;

$\mathfrak{Ю}^{н}$ — множество реализуемых требований к надежностным характеристикам КСА;

$\mathfrak{Ю}^{н}_{тр}$ — множество заданных требований к надежностным характеристикам КСА;

M — множество предприятий-исполнителей работ по созданию (развитию) АСУ СН;

$W_j(X(u), Y(u), Z(u))$ — необходимые технологические возможности j-го предприятия-исполнителя на выполнение работ по созданию (развитию) АСУ СН;

$W^{доп}j(u)$ — допустимые технологические возможности j-го предприятия-исполнителя на выполнение работ по созданию (развитию) АСУ СН;

R — риск несвоевременного выполнения решений по созданию (развитию) АСУ СН;

$R^{р}_{доп}$ — допустимый риск реализации решений по разработке КСА;

$R^{и}_{доп}$ — допустимый риск реализации решений по изготовлению КСА и оснащению ОУ;

C — стоимость реализации решений по созданию (развитию) АСУ СН;

$C_{доп}(u)$ — финансовые ограничения на создание (развитие) АСУ СН;

T — продолжительность выполнения работ по созданию (развитию) АСУ СН;

$T_{доп}(u)$ — длительность ЭП.

Оценка алгоритмической сложности для одного частного случая поставленной задачи (1), проведенная в [2], позволяет сделать вывод о том, что применение точных методов для ее решения возможно только для небольших размерностей исходных данных. В то же время следует учитывать, что на начальных этапах проектирования АСУ СН входные данные для выбора решений по созданию (развитию) АСУ СН могут быть определены неточно. Поэтому, как показано в [2], для решения поставленной задачи возможным и целесообразным является использование «жадных» алгоритмов.

Ряд подходов к оценке эффективности АСУ СН на различных стадиях жизненного цикла изложен в [3, 11, 12].

В качестве показателя эффективности выполнения ФП $E(X(u), Y(u), Z(u))$ может быть применен обобщенный показатель функциональной эффективности [3], характеризующий полноту реализации ФП, их важность, а также своевременность, достоверность и точность их реализации в АСУ СН.

Алгоритм выбора решений
по созданию (развитию) АСУ СН

Научно-методический аппарат формирования, оценки и выбора решений по созданию (развитию) АСУ СН для одного частного случая поставленной задачи (1) приведен в [2]. На его основе ниже предложен «жадный» алгоритм, учитывающий особенности поставленной задачи оптимизации.

Формирование решений по разработке и изготовлению КСА и оснащению ими ОУ АСУ СН, а также о планируемых работах по продлению эксплуатации КСА предлагается осуществлять следующим образом.

1. Ввод исходных данных. Оценка их полноты и непротиворечивости.

2. Создание директивно заданных решений на изготовление серийных КСА, разработку и изготовление перспективных КСА.

3. Расчет приоритетов всех ОУ в соответствии с методом формирования приоритетного перечня ОУ, подлежащих оснащению средствами автоматизации, изложенным в [4].

4. Сортировка ОУ по убыванию приоритета.

5. Выбор очередного ОУ.

6. Проверка отсутствия директивно заданной работы на изготовление серийного КСА для выбранного ОУ. В случае невыполнения данного условия осуществляется переход к п. 23.

7. Проверка, что установленный на ОУ КСА не обеспечивает решение всех ФЗ из состава ФПв для выбранно-

го ОУ. В случае невыполнения данного условия осуществляется переход к п. 23.

8. Проверка существования серийных КСА для выбранного ОУ. В случае невыполнения данного условия осуществляется переход к п. 13.

9. Формирование списка серийных КСА, обеспечивающих решение всех ФЗ из состава ФПв для выбранного ОУ.

10. В случае, если выбранный ОУ возможно оснастить несколькими серийными КСА, выбирается КСА с минимальной стоимостью изготовления. При выборе КСА проверяется выполнимость заданных в задаче (1) требований и ограничений.

11. Если КСА не может быть выбран, осуществляется переход к п. 13.

12. Создание работы на изготовление серийного КСА для выбранного ОУ.

13. Проверка отсутствия созданных работ на разработку перспективного КСА для выбранного ОУ. В случае невыполнения данного условия осуществляется переход к п. 20.

14. Проверка существования перспективных КСА для выбранного ОУ. В случае невыполнения данного условия осуществляется переход к п. 23.

15. Формирование списка перспективных КСА, обеспечивающих решение всех ФЗ из состава ФПв для выбранного ОУ.

16. В случае, если выбранный ОУ возможно оснастить несколькими перспективными КСА, выбирается КСА с минимальной стоимостью разработки и изготовления. При выборе КСА проверяется выполнимость заданных в задаче (1) требований и ограничений.

17. Если КСА не может быть выбран, осуществляется переход к п. 23.

18. Создание работы на разработку перспективного КСА для выбранного ОУ

19. Создание работы на изготовление перспективного КСА для выбранного ОУ.

20. Проверка отсутствия созданных работ на изготовление перспективного КСА для выбранного ОУ. В случае невыполнения данного условия осуществляется переход к п. 23.

21. Проверка возможности создания работы на изготовление перспективного КСА для выбранного ОУ. При невозможности создания работы осуществляется переход к п. 23.

22. Создание работы на изготовление перспективного КСА для выбранного ОУ

23. Если остались нерассмотренные ОУ, то осуществляется переход к п. 5.

24. Расчет приоритетов всех ОУ в соответствии с методом формирования приоритетного перечня ОУ, подлежащих оснащению средствами автоматизации, изложенным в [4] с учетом созданных работ.

25. Сортировка ОУ по убыванию приоритета.

26. Выбор очередного ОУ.

27. Проверка отсутствия созданных работ на разработку и изготовление перспективного КСА для выбранного ОУ. В случае невыполнения данного условия осуществляется переход к п. 31.

28. Проверка отсутствия созданной работы на изготовление серийного КСА для выбранного ОУ. В случае невыполнения данного условия осуществляется переход к п. 34.

29. Проверка, что установленный на ОУ КСА не обеспечивает решение всех ФЗ из состава ФПв для выбранного ОУ. В случае невыполнения данного условия осуществляется переход к п. 40.

30. Для заданных исходных данных и ограничений отсутствует решение задачи (1). Конец работы алгоритма.

31. Оценка возможности изменения работ на разработку и изготовление выбранного перспективного КСА на перспективный КСА, обеспечивающий решение всех ФЗ для выбранного ОУ.

32. Если изменение работ невозможно, осуществляется переход к п. 46.

33. Изменение работ на разработку и изготовление выбранного перспективного КСА на перспективный КСА, обеспечивающий решение всех ФЗ для выбранного ОУ. Переход к п. 46.

34. Оценка возможности изменения работы на изготовление выбранного серийного КСА на серийный КСА, обеспечивающий решение всех ФЗ для выбранного ОУ.

35. Если изменение работы невозможно, осуществляется переход к п. 37.

36. Изменение работы на изготовление выбранного серийного КСА на серийный КСА, обеспечивающий решение всех ФЗ для выбранного ОУ. Переход к п. 46.

37. Оценка возможности изменения работы на изготовление выбранного серийного КСА на разработку и изготовление перспективного КСА, обеспечивающий решение всех ФЗ для выбранного ОУ.

38. Если изменение работы невозможно, осуществляется переход к п. 46.

39. Изменение работы на изготовление выбранного серийного КСА на разработку и изготовление перспективного КСА, обеспечивающий решение всех ФЗ для выбранного ОУ. Переход к п. 46.

40. Оценка возможности создания работы на изготовление серийного КСА, обеспечивающего решение всех ФЗ для выбранного ОУ.

41. Если создание работы невозможно, осуществляется переход к п. 43.

42. Создание работы на изготовление серийного КСА, обеспечивающего решение всех ФЗ для выбранного ОУ. Переход к п. 46.

43. Оценка возможности создания работ на разработку и изготовление перспективного КСА, обеспечивающий решение всех ФЗ для выбранного ОУ.

44. Если создание работ невозможно, осуществляется переход к п. 46.

45. Создание работ на разработку и изготовление перспективного КСА, обеспечивающий решение всех ФЗ для выбранного ОУ.

46. Если остались нерассмотренные ОУ, то переход к п. 26.

47. Для заданных исходных данных и ограничений решение задачи (1) сформировано. Конец работы алгоритма.

Схема алгоритма представлена на рис. 2.

Программные средства выбора решений по созданию (развитию) АСУ СН

Следует отметить, что использование формализованных подходов для выбора решений по созданию (развитию) АСУ СН предполагает необходимость сбора, хранения и обработки массивов исходных данных, объем которых зависит от размерности, а также параметров организационной и функциональной структуры рассматриваемой системы управления [17–20]. Очевидным путем для сокращения трудозатрат на обработку этих данных является использование специализированных программно-инструментальных средств. Кроме того, это позволит минимизировать количество ошибок, связанных с вводом и обработкой информации. В связи с этим, авторами разработан программный комплекс поддержки принятия решений по созданию (развитию) АСУ СН, позволяющий в автоматизированном режиме формировать рациональный вариант решений по разработке, изготовлению и продлению эксплуатации КСА для ОУ из состава АСУ СН.

Основными функциональными возможностями данного программного комплекса являются:

1) Ввод, отображение, редактирование и хранение данных о состоянии и требованиях к автоматизации АСУ СН. Программный комплекс позволяет задавать организационную и функциональную структуру АСУ СН, перечень и характеристики существующих и перспективных КСА, требования к реализации функциональных подсистем, процессов и задач.

2) Ввод, отображение, редактирование и хранение данных о планируемых работах (НИОКР по разработке КСА, о планируемых работах по изготовлению КСА и оснащению ими ОУ из состава АСУ СН, а также о планируемых работах по обеспечению эксплуатации и продлению ресурса КСА на ОУ).

3) Автоматизированное формирование приоритетного перечня ОУ из состава АСУ СН на основе последовательной оценки каждого из них в соответствии с предложенной системой классификационных признаков.

4) Автоматизированное формирование решений по разработке и изготовлению КСА, оснащению ими ОУ из состава АСУ СН, а также о планируемых работах по обеспечению эксплуатации и продлению ресурса КСА на ОУ. Программный комплекс позволяет формировать перечень и характеристики вышеуказанных работ в условиях финансовых, временных и технологических ограничений на основе использования предложенного выше алгоритма максимального элемента.

5) Отображение результатов выбора решений для каждого планового этапа (данных о планируемых НИОКР по разработке и изготовлению КСА и оснащению ими ОУ из состава АСУ СН, а также о планируемых работах по обеспечению эксплуатации и продлению ресурса КСА на ОУ. Программный комплекс позволяет отображать указанные данные в виде таблиц и иерархической диаграммы с указанием состояния КСА для каждого ОУ на каждом плановом этапе для рассматриваемого периода прогноза).

В программном комплексе реализовано 4 основных функциональных блока, которые соответствуют пунктам главного меню:

1) Администрирование программного комплекса.

2) Ведение справочников и классификаторов.

3) Ввод и отображение исходных данных.

4) Формирование и отображение результатов решения.

Ниже рассмотрим сущность каждого из указанных пунктов главного меню программного комплекса.

1) Администрирование программного комплекса.

В пункте «Администрирование» реализованы все функции по настройке программного комплекса, включая настройку вида экранных форм и отображаемых отчетов, а также функции разграничения доступа.

2) Ведение справочников и классификаторов.

В пункте «Справочники» реализованы функции по ведению массивов условно-постоянной информации, а именно:

– типы органов управления;

– важность реализуемых в системе управления функциональных подсистем, процессов и задач;

– стадии жизненного цикла КСА;

– типы работ, к которым относятся разработка КСА, их изготовление и продление эксплуатации;

– назначение организации, определяющее, какие виды работ может выполнять организация — разработчик, изготовитель, эксплуатирующая организация.

В указанных экранных формах возможно добавление, удаление и редактирование соответствующих данных.

3) Ввод и отображение исходных данных.

3.1) *Форма «Проект»*

Проект представляет собой полный набор данных, необходимых для выполнения расчетов по конкретной системе управления. Одновременно в программном комплексе могут храниться данные по нескольким исследуемым системам управления.

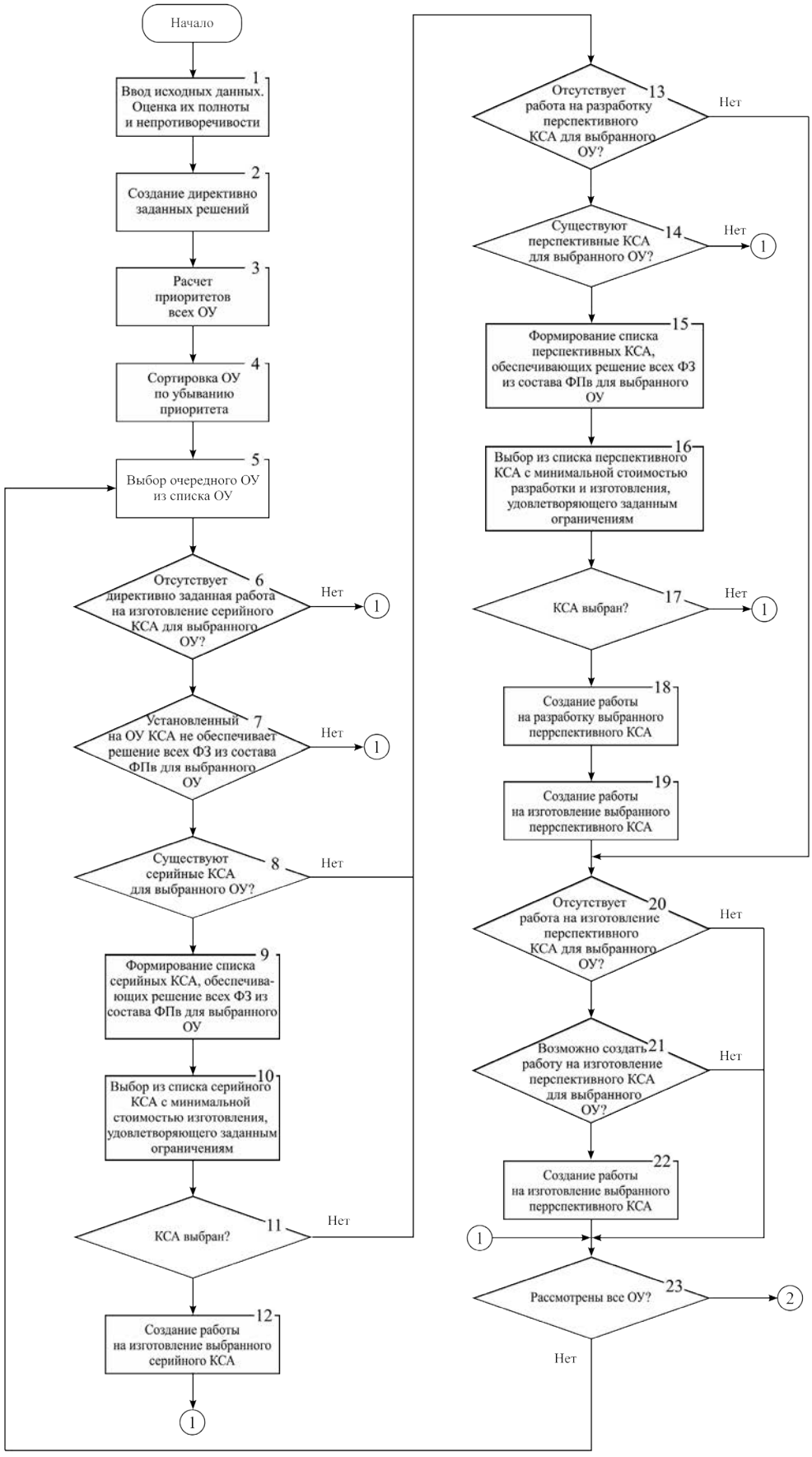


Рис. 2. Алгоритм выбора решений по созданию (развитию) АСУ СН (начало)

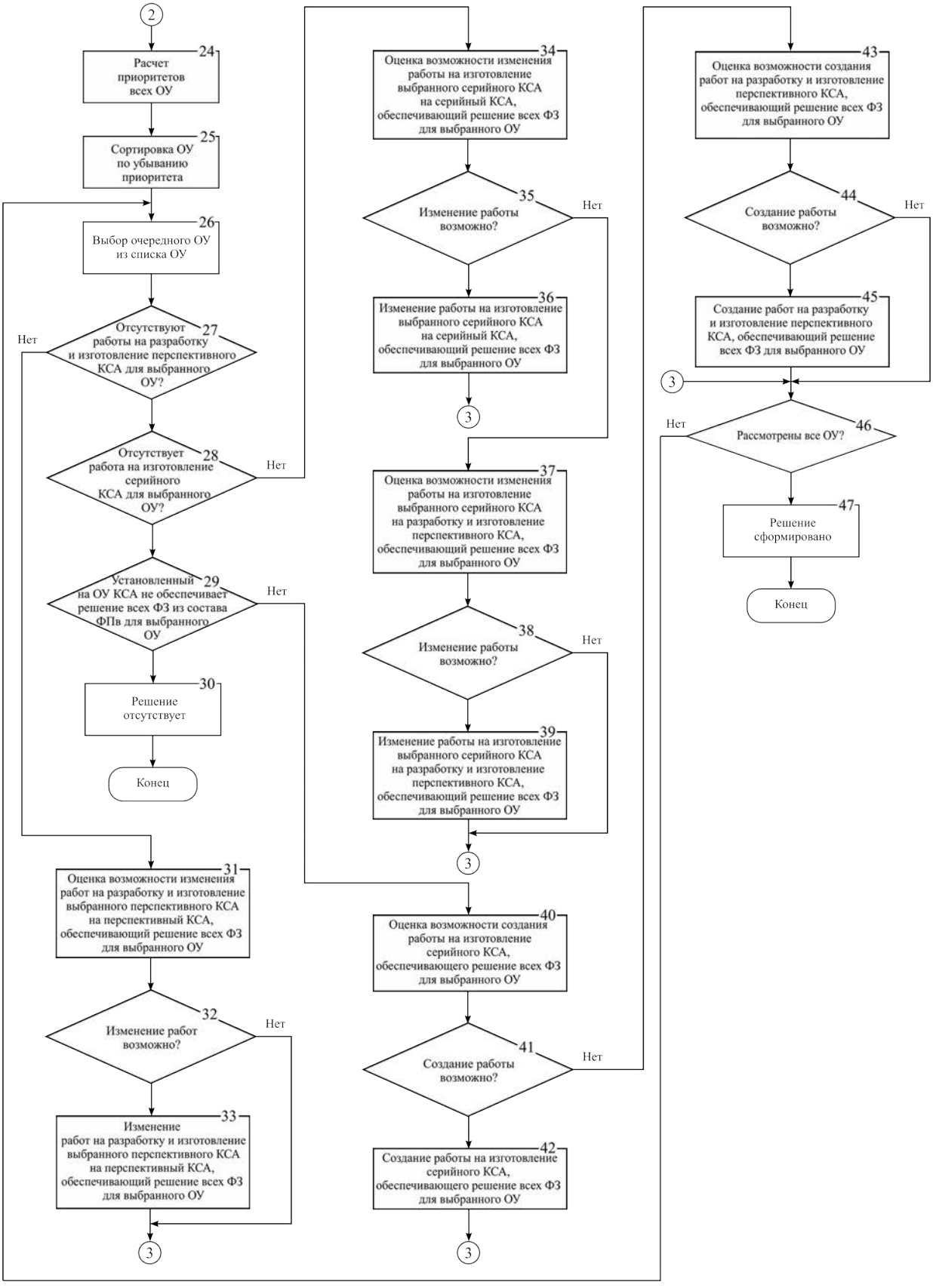


Рис. 2. Алгоритм выбора решений по созданию (развитию) АСУ СН (окончание)

3.2) *Форма «Подсистемы АСУ — Процессы АСУ — Задачи типов ОУ»*

Данная форма обеспечивает ввод и редактирование информации о функциональной структуре системы управления, состоящей из функциональных подсистем, процессов и задач. Для упрощения ввода больших массивов данных реализована возможность копирования подсистем, процессов и задач, а также дальнейшего редактирования этой информации.

3.3) *Форма «Предприятие»*

Форма предназначена для ввода сведений по предприятию. Во вкладке «Назначение» возможно выбирать несколько из заданных вариантов его назначения. В зависимости от этих свойств каждое предприятие может быть исполнителем только определенных типов работ.

3.4) *Форма «Информация о КСА»*

Форма предназначена для ввода информации о КСА. При этом указываются стоимостные и временные параметры работ по разработке, изготовлению, обеспечению эксплуатации и продлению ресурса КСА на ОУ. Также указывается, какие функциональные задачи реализованы, а какие могут быть реализованы в КСА. Кроме того, реализованы функции по добавлению, удалению и редактированию информации о КСА.

3.5) *Форма «Органы управления»*

Форма предназначена для ввода и редактирования информации об организационной структуре системы управления.

В левой части представлена иерархическая структура ОУ с возможностью добавления, удаления и редактирования информации по ОУ.

По каждому ОУ указываются его основные признаки, которые используются для определения приоритетов оснащения ОУ, а также информация о КСА, находящемся на эксплуатации.

3.6) *Форма «Этапы прогнозирования»*

Форма предназначена для ввода информации по этапам прогнозирования. Как правило, в качестве этапа целесообразно рассматривать календарный год. Реализована возможность добавления, изменения, удаления этапа, а также отображения данных по привязке конкретных работ к этапам прогнозирования.

4) Формирование и отображение результатов решения.

4.1) *Форма «Решения»*

В данной экранной форме (рис. 3) в табличном виде отображается результат решения задачи выбора системотехнических решений по созданию (развитию) АСУ СН в виде перечня работ по разработке, изготовлению, обеспечению эксплуатации и продлению ресурса КСА на ОУ. При этом указывается, какая работы должна выполняться конкретным предприятием промышленности с привязкой к этапам прогнозирования.

Также здесь реализована возможность ввода и отображения информации по директивно задаваемым оператором решениям (опорным решениям) по разработке, изготовлению, обеспечению эксплуатации и продлению ресурса КСА на ОУ КСА.

4.2) *Форма «Отчеты»*

Данная форма (рис. 4) предназначена для отображения значений показателей эффективности, характеризующих сформированные решения, а также цветовой индикации степени оснащенности ОУ в зависимости от количества реализованных в КСА функциональных задач.

В качестве обобщенного показателя эффективности принятых решений по созданию (развитию) АСУ СН принято значение показателя целевой функции из задачи (1).

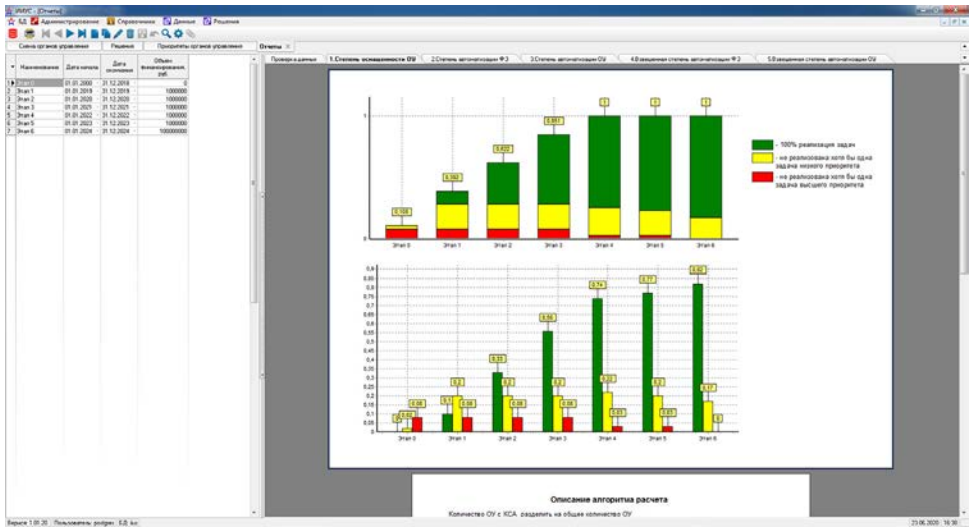


Рис. 4. Экранная форма «Отчеты»

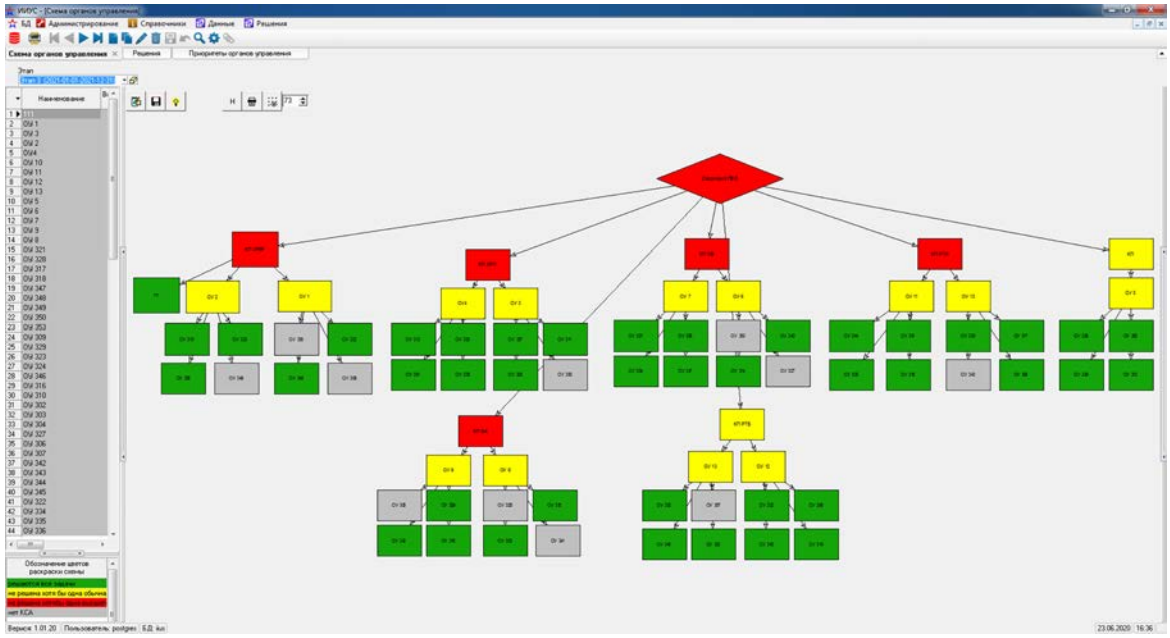


Рис. 6. Экранная форма «Схема органов управления»

В качестве частных показателей эффективности приняты следующие частные показатели, характеризующие степень оснащенности ОУ и степень автоматизации АСУ СН [3]:

– степень оснащенности ОУ;
– степень автоматизации ФЗ;
– степень автоматизации ОУ;
– взвешенная степень автоматизации ФЗ;
– взвешенная степень автоматизации ОУ.

4.3) *Форма «Схема органов управления»*

Данная форма (рис. 5) предназначена для отображения организационной структуры системы в виде графической схемы с цветовым обозначением полноты автоматизированного решения задач на ОУ. Здесь реализована возможность добавления и удаления ОУ со схемы, изменения местоположения ОУ, цветовой индикации степени автоматизации ОУ в зависимости от выбранного этапа, а также изменения масштаба отображения.

На основные компоненты разработанного программного комплекса получены свидетельства о государственной регистрации программы для ЭВМ № 2018660348, 2018662688, 2018666516, 2019612091, 2019614502, 2020612350.

Заключение

Предложенные в статье метод и реализующий его алгоритм позволяют автоматизировать процессы подготовки исходных данных и выбора решений по созданию (развитию) АСУ СН, что обеспечит сокращение трудоемкости и унификацию процедур подготовки плановых организационных и финансовых документов при обосновании федеральных и ведомственных целевых программ по разработке и модернизации распределенных информационно-управляющих систем специального назначения.

Литература

1. *Alasheev M.A., Bresler I.B., Lyaskovskii V.L.* Methods and models for decision-making in systems engineering for creating (developing) distributed organizational information and control systems // Journal of Computer and Systems Sciences International. 2020. Vol. 59. No 2. Pp. 245–260.

2. *Lyaskovsky V.L., Bresler I.B., Alasheev M.A.* The approaches to developing the distributed information-control systems of organizational type // ITM Web of Conferences. 2018. Vol. 18. P. 01005.

3. *Элькин Г.И., Лясковский В.Л., Алашеев М.А.* Показатели и методы оценки функциональной эффективности распределенных информационно-управляющих систем организационного типа // Вестник ТвГУ. Серия: Прикладная математика. 2019. № 3. С. 40–52.

4. *Лясковский В.Л., Бреслер И.Б., Алашеев М.А.* Метод формирования приоритетного перечня автоматизируемых органов управления в системах специального назначения и его программная реализация // Программные продукты и системы. 2019. Т. 32. № 4. С. 708–713.

5. *Haass O., Azizi N.* Challenges and solutions across project life cycle: a knowledge sharing perspective // International Journal of Project Organisation and Management. 2020. Vol. 12. No. 4. Pp. 346–379. doi:10.1504/IJPOM.2020.111067.

6. *Paul P.K.* Information System and Its Types: Emphasizing Territory, Establishments and Domain Specific // TechnoLearn: An International Journal of Educational Technology. 2020. Vol. 10. No. 1&2. Pp. 39–48. doi:10.30954/2231–4105.02.2020.6.

7. *Егоров Ю.П., Пятаков А.И., Сулейманова Л.И.* Оценка готовности программно-технического комплекса к решению функциональных задач // Автоматизация процессов управления. 2018. № 2 (52). С. 20–27.

8. *Третьяков В.А., Куликов Г.В., Лукьянец Ю.Ф.* Принципы построения больших территориально распределенных автоматизированных систем // Российский технологический журнал. 2020. № 8 (1). С. 34–42.

9. *Hughes D.L., Rana N.P., Simintiras A.C.* The changing landscape of IS project failure: an examination of the key factors // Journal of Enterprise Information Management. 2017. Vol. 30. No. 1. Pp. 142–165. doi:10.1108/JEIM-01–2016–0029.

10. *Горелов Б.А., Давыдов А.Д., Силаев А.В., Тихонов А.В.* Модели управления развитием распределенных технических систем // Известия высших учебных заведений. Машиностроение. 2018. № 3 (696). С. 92–103.

11. *Зальмарсон А.Ф., Васильев В.А., Елецкий М.И., Сидоров С.С.* Общесистемные показатели эффективности автоматизированных систем управления (программно-аппаратных комплексов) // Автоматизация процессов управления. 2018. № 3 (53). С. 11–19.

12. *Зацаринный А.А. Ионенков Ю.С.* Некоторые аспекты оценки эффективности автоматизированных информационных систем на различных стадиях их жизненного цикла // Системы и средства информатики. 2016. Т. 26. № 3. С. 121–135.

13. *Матвиенко Ю.А.* Направления развития автоматизированных систем управления военного назначения на основе принципа сбалансированности // Военная мысль. 2020. № 2. С. 81–88.

14. *Козлов С.В.* Процессные аспекты повышения качества создания интеллектуальных интегрированных систем управления // Надежность и качество сложных систем. 2020. № 4 (32). С. 22–30. doi:10.21685/2307–4205–2020–4–3.

15. *Kozlov S.V., Kubankov A.N.* Scientific and methodical aspects of synchronization of functional processes in the life cycle of integrated control systems // Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO). 2019. Pp. 1–5. doi: 10.1109/SYNCHROINFO.2019.8813991.

16. *Легков К.Е.* Методические основы управления информационными подсистемами автоматизированных систем управления сложными объектами специального назначения // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 5. С. 31–40. doi:10.24411/2072–8735–2018–10084.

17. *Бригаднов С.И.* Разработка комплексной автоматизированной интеллектуальной системы анализа проектных решений и обучения проектировщика // V Международная научно-практическая конференция «Электронное обучение в непрерывном образовании 2018». Ульяновск, 2018. С. 136–142.

18. *Elnagar S., Weistroffer H.R.* Introducing Knowledge Graphs to Decision Support Systems Design // Information Systems: Research, Development, Applications, Education. 2019. Vol. 359. Pp. 3–11. doi: 10.1007/978–3–030–29608–7_1.

19. *Flores-Garcia E., Bruch J., Wiktorsson M., Jackson M.* Decision-making approaches in process innovations: an explorative case study // Journal of Manufacturing Technology Management. 2019. Vol. 32. No. 9. Pp. 1–25. doi:10.1108/JMTM-03–2019–0087.

20. *Grange C., Pinsonneault A.* The Responsible Adoption of (Highly) Automated Decision-Making Systems // Proceedings of the 54th Hawaii International Conference on System Sciences. Hawaii, 2021. Pp. 4900–4909. doi:10.24251/HICSS.2021.595.

METHODOLOGICAL AND SOFTWARE TOOLS FOR SELECTING SOLUTIONS FOR THE CREATION (DEVELOPMENT) OF AUTOMATED CONTROL SYSTEMS

VIKTOR L. LYASKOVSKIY
Tver, Russia, dop_big@mail.ru

IGOR B. BRESLER
Tver, Russia, niiit@niiit.tver.ru

MIKHAIL A. ALASHEEV
Tver, Russia, mihal81@mail.ru

KEYWORDS: automated control system for special purposes; automation complex; selection of solutions for the creation and development of automated control systems; efficiency of the automated control system; decision support software package.

ABSTRACT

Introduction: to date, the issues of substantiation, assessment and choice of options for the creation (development) of automated control systems for special purposes are not formalized enough and do not allow the selection of solutions to comprehensively take into account the totality of a number of significant parameters: prescriptive decisions; classification signs of command centers; functional processes of the highest priority; specified maximum permissible probabilistic-temporal and temporal characteristics of the performance of functional processes; information security requirements; design and reliability requirements; technological capabilities of executing enterprises; acceptable time and cost parameters of the system creation process; risks of untimely implementation of solutions for the development, manufacture of automation equipment and equipping command centers with them. **Purpose:** development of methodological and software tools for choosing solutions for the creation (development) of special-purpose automated control systems that maximize the

efficiency of performing functional processes in the system, taking into account the specified requirements and restrictions. **Methods:** methodological tools are proposed, including the formalization of the structure of automated control systems for special purposes, the formulation of the problem of choosing solutions for their creation (development), as well as an algorithm for solving the problem, based on the use of "greedy" methods of discrete optimization. **Results:** the developed methodological tools are implemented in the form of specialized software tools, which are the basis of the decision support software complex, which allows to find a solution to the problem in an automated mode, namely, to form a rational solution for the development, manufacture and prolongation of the operation of automation systems for command centers from the composition of automated systems management of special purpose. **Practical relevance:** the research results can be used to substantiate federal and departmental target programs for the development and modernization of distributed information and control systems for special purposes. **Discussion:** the use of the developed methodological and software tools will increase the validity and reduce the labor intensity of the processes of forming decisions for the creation (development) of automated control systems for special purposes.

REFERENCES

1. Alasheev M.A., Bresler I.B., Lyaskovskii V.L. Methods and models for decision-making in systems engineering for creating (developing) distributed organizational information and control systems. *Journal of Computer and Systems Sciences International*. 2020. Vol. 59. No 2. Pp. 245–260.

2. Lyaskovsky V.L., Bresler I.B., Alasheev M.A. The approaches to developing the distributed information-control systems of organizational type. *ITM Web of Conferences*. 2018. Vol. 18. P. 01005.

3. Elkin G.I., Lyaskovsky V.L., Alasheev M.A. Indicators and methods for assessing the functional effectiveness of distributed information management systems of an organizational type. *Vestnik TvGU. Seriya: Prikladnaya matematika* [Herald of Tver State University. Series: Applied Mathematics]. 2019. No. 3. Pp. 40–52. (In Rus)

4. Lyaskovsky V.L., Bresler I.B., Alasheev M.A. The method of formation of the priority list of automated control centers in special purpose systems and its software implementation. *Programmnye produkty i sistemy* [Software & Systems]. 2019. No. 4. Pp. 708–713. (In Rus)

5. Haass O., Azizi N. Challenges and solutions across project life cycle: a knowledge sharing perspective. *International Journal of Project Organisation and Management*. 2020. Vol. 12. No. 4. Pp. 346–379. doi:10.1504/IJPOM.2020.111067

6. Paul P.K. Information System and Its Types: Emphasizing Territory, Establishments and Domain Specific. *TechnoLearn: An International Journal of Educational Technology*. 2020. Vol. 10. No. 1&2. Pp. 39–48. doi:10.30954/2231–4105.02.2020.6

7. Egorov I.P., Piatakov A.I., Suleimanova L.I. Estimation of hardware and software complex readiness to solve the functional tasks. *Avtomatizacija processov upravlenija* [Automation of Control Processes]. 2018. No. 2 (52). Pp. 20–27. (In Rus).

8. Tretyakov A.V., Kulikov G.V., Lukyanets Y.F. Principles of creation of the big territorially distributed automated systems. *Rossiyskiy tekhnologicheskiy zhurnal* [Russian Technological Journal]. 2020. No. 8. Pp. 34–42. (In Rus)

9. Hughes D.L., Rana N.P., Simintiras A.C. The changing landscape of IS project failure: an examination of the key factors. *Journal of Enterprise Information Management*. 2017. Vol. 30. No. 1. Pp. 142–165. doi:10.1108/JEIM-01–2016–0029

10. Gorelov B.A., Davydov A.D., Silaev A.V., Tihonov A.V. Models of development management of distributed technical systems. *Izvestiya vysshikh uchebnykh zavedeniy. Mashinostroenie* [University news. Engineering]. 2018. No. 3 (696). Pp. 92–103. (In Rus)

11. Zalmarson A.F., Vasilev V.A, Eletskii M.I., Sidorov S.S. System-wide performance indicators of automated command and control systems (software-hardware complexes). *Avtomatizacija processov upravlenija* [Automation of Control Processes]. 2018. No. 3 (53). Pp. 11–19. (In Rus)

12. Zatsarinny A.A., Ionenkov J.S. Some aspects of evaluating the effectiveness of automated information systems at various stages of their life cycle. *Sistemy i sredstva informatiki* [Systems and means of informatics]. 2016. Vol. 26. No. 3. Pp. 121–135. (In Rus)

13. Matvienko Y.A. Development trends in military automated control systems based on the balance principle. *Voennaja mysl* [Military Thought]. 2020. No. 2. Pp. 81–88. (In Rus)

14. Kozlov S.V. Process aspects of improving the quality of creating intelligent integrated management systems. *Nadezhnost i kachestvo slozhnyh sistem* [Reliability and quality of complex systems]. 2020. No. 4 (32). Pp. 22–30. (In Rus). doi:10.21685/2307–4205–2020–4–3

15. Kozlov S.V., Kubankov A.N. Scientific and methodical aspects of synchronization of functional processes in the life cycle of integrated control systems. *Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)*. 2019. Pp. 1–5. doi: 10.1109/SYNCHROINFO.2019.8813991

16. Legkov K.E. Methodical foundations of management of information subsystems of automated control systems for complex objects of special purposes. *T-Comm*. 2018. Vol. 12. No. 5. Pp. 31–40. (In Rus).

17. Brigadnov S.I. Razrabotka kompleksnoj avtomatizirovannoj intellektualnoj sistemy analiza proektnyh reshenij i obuchenija proektirovshhika [Development of complex automated system of intellectual analysis of design solutions and training designer]. *V Mezhdunarodnaja nauchno-prakticheskaja konferencija "Jelektronnoe obuchenie v nepreryvnom obrazovanii 2018"* [V International Scientific and Practical Conference "E-Learning in Continuing Education 2018"]. Ulyanovsk, 2018. Pp. 136–142. (In Rus)

18. Elnagar S., Weistroffer H.R. Introducing Knowledge Graphs to Decision Support Systems Design. *Information Systems: Research, Development, Applications, Education*. 2019. Vol. 359. Pp. 3–11. doi: 10.1007/978–3–030–29608–7_1

19. Flores-Garcia E., Bruch J., Wiktorsson M., Jackson M. Decision-making approaches in process innovations: an explorative case study. *Journal of Manufacturing Technology Management*. 2019. Vol. 32. No. 9. Pp. 1–25. doi:10.1108/JMTM-03–2019–0087

20. Grange C., Pinsonneault A. The Responsible Adoption of (Highly) Automated Decision-Making Systems. *Proceedings of the 54th Hawaii International Conference on System Sciences*. Hawaii, 2021. Pp. 4900–4909. doi:10.24251/HICSS.2021.595

INFORMATION ABOUT AUTHORS:

Lyaskovskiy V.L., PhD, Full Professor, Chief Research Officer of the Research Institute of Information Technologies;

Bresler I.B., PhD, Docent, Director of the Research Institute of Information Technologies;

Alasheev M.A., PhD, Scientific Coordination Department Specialist of the Research Institute of Information Technologies.

For citation: Lyaskovskiy V.L., Bresler I.B., Alasheev M.A. Methodological and software tools for selecting solutions for the creation (development) of automated control systems. *H&ES Research*. 2021. Vol. 13. No. 3. Pp. 48–59. Doi: 10.36724/2409-5419-2021-13-3-48-59 (In Rus)

Doi: 10.36724/2409-5419-2021-13-3-60-67

МОДЕЛЬ КАНАЛА НЕСАНКЦИОНИРОВАННОГО ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ

СИНЮК
Александр Демьянович[1]

ОСТРОМОВ
Олег Александрович[2]

АННОТАЦИЯ

Введение. Большие объемы конфиденциальной информации пользователей хранятся в информационных системах на накопителях с жесткими магнитными дисками. Удаление файлов пользователей средствами операционной системы с магнитного накопителя оставляет для нарушителя возможность их восстановления посредством современных технологий. Известные методы уничтожения информации не отвечают требованиям оперативности, экономичности, безопасности. **Цель исследования:** разработка адекватной модели канала несанкционированного восстановления информации в условиях использования нарушителем современной и максимально эффективной технологии восстановления удаленных информационных данных. **Методы:** анализ известных методов восстановления информации в современных условиях непрерывного увеличения плотности записи информации на накопители позволил выделить наиболее совершенный метод магнитной сканирующей микроскопии, отличающийся очень высокой разрешающей способностью исследования областей остаточной намагниченности магнитных накопителей после удаления информации. **Результаты:** сделано предположение, что нарушитель в совершенстве владеет технологией магнитной сканирующей микроскопии и имеет возможности ее применения для восстановления данных, удаленных пользователем. Анализ принципов работы современных магнитных сканирующих микроскопов позволил оценить вероятности ошибочного декодирования и среднего числа ошибок в восстановленном информационном блоке, а также создать условия для разработки адекватной модели канала несанкционированного восстановления информации, которая включает источник информации, представляющий собой поверхность магнитного накопителя, и оборудование нарушителя для доступа к остаточной информации. Источник с приемником (оборудованием нарушителя) связывает канал передачи (считывания) информации, который на основе проведенного анализа предложено описать моделью двоичного симметричного канала. **Практическая значимость:** представленную модель канала нарушителя предлагается использовать для разработки адекватного требованиям метода надежного уничтожения конфиденциальной информации пользователя с магнитного накопителя. **Обсуждение:** результаты рекомендуются специалистам информационных систем, включающих подсистему защиты информации от несанкционированного доступа для синтеза адекватной модели нарушителя, а также разработки, селекции и оценки безопасности новых методов уничтожения конфиденциальной информации.

КЛЮЧЕВЫЕ СЛОВА: накопители на жестких магнитных дисках; удаление конфиденциальной информации; области остаточной намагниченности; нарушитель; магнитная силовая микроскопия; канал несанкционированного восстановления информации; модель двоичного симметричного канала без памяти.

Сведения об авторах:

[1]д.т.н., доцент, профессор Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия, eentrop@rambler.ru

[2]к.т.н., докторант Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия, oleg-26stav@mail.ru

Для цитирования: *Синюк А.Д., Остроумов О.А.* Модель канала несанкционированного восстановления информации // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13. № 3. С. 60–67. Doi: 10.36724/2409-5419-2021-13-3-60-67

Введение

В современных информационных системах большие объемы информации хранятся на энергонезависимых носителях. К этому типу относятся накопители на жестких магнитных дисках (НЖМД). Информация имеет много этапов жизненного цикла информации. Некоторые из этапов создают предпосылки для несанкционированного доступа (НСД) к конфиденциальной информации [1–3]. Особенно выделяется этап надежного удаления критичной информации с накопителя [4–6].

Удаление файлов штатными средствами операционной системы или переформатирование НЖМД практически не удаляет данные. Это связано с тем, что при удалении файла с закрытой информацией штатными средствами файловой системы ПЭВМ сама информация не перезаписывается. Драйвер отмечает, что соответствующая файловая запись не используется и, соответственно, сектора накопителя, содержавшие данные удаленного файла становятся свободными для записи новой информации. В условиях, когда данные файлов удаленные таким образом не будут перезаписаны, то существует возможность их восстановить и считать с накопителя [5–7].

Можно выделить два основных пути или канала утечки остаточной информации, возникающей вследствие ее недостаточно надежного удаления с НЖМД [1, 3].

Первым из них является утечка информации при замене НЖМД. В этих случаях старые компьютеры вывозятся вместе с носителями информации, а значит и со всеми данными.

В то время как существуют не только законы, но и аппаратные и программные средства, запрещающие или препятствующие получению конфиденциальной информации, снятие данных со списанного НЖМД позволяет заинтересованному лицу не только обойти системы безопасности без риска быть обнаруженным, но и сделать это практически законно [1, 2]. Простое удаление файлов или даже переформатирование жесткого диска фактически не удаляет информацию. Запись поверх удаляемой информации новых данных так же не дает полной гарантии ее уничтожения. Это обусловлено тем, что траектория движения записывающей головки жесткого диска не совпадает с магнитной дорожкой абсолютно точно. По краям дорожек имеются области остаточной намагниченности, несущие информацию о предыдущих записях. Стоит записать информацию на НЖМД и удалить ее из магнитной памяти диска будет очень сложно. Поэтому, казалось бы, безвредный акт списания старого компьютера или передача его в другую организацию — наиболее простой путь несанкционированного получения информации с ограниченным доступом [3, 5].

Кроме той конфиденциальной информации, о которой знают пользователи (бухгалтерской, финансовой, личной, перспективных разработках), на ПК может храниться множество других конфиденциальных данных, которые не всегда известны оператору. Приложения и операционные системы хранят пароли, ключи шифрования и другие данные с ограниченным доступом в различных местах, включая файлы конфигурации и временные файлы. Операционные системы произвольным образом записывают содержимое памяти в файл подкачки на диске, что не дает возможности узнать, что из этих данных действительно сохранено на носителе [1–3].

Вторым каналом утечки информации являются неисправные накопители. В 56% случаев потери данных связаны с аппаратными сбоями НЖМД [2, 5].

Технологии хранения информации на магнитных носителях развиваются очень быстро. На современных НЖМД хранится в 500 раз больше информации, чем 10 лет назад. Значительно увеличилась плотность записи информации и скорость вращения магнитных пластин, но, к сожалению, такой показатель НЖМД, как надежность, ухудшился [5]. Так, практически все производители дисков перешли с 3-х годичной гарантии на одногодичную.

Многие диски выходят из строя в гарантийный период и могут быть заменены по гарантии при условии сохранности пломб и отсутствии механических повреждений или следов вскрытия. При этом считать информацию с диска, переписать ее на другой носитель или стереть не предоставляется возможным по причине неисправности НЖМД. Жесткий диск с информацией обменивается фирмой-продавцом на новый накопитель, а неисправный отсылается производителю или переводится на длительное хранение. В большинстве случаев причина выхода НЖМД из строя — неисправность механики или контроллера, которые могут легко быть заменены или отремонтированы на заводе-производителе или в специализированном сервисном центре, которые находятся за рубежом. В результате огромное количество информации, в том числе и конфиденциальной, попадает в руки посторонних лиц [2, 3, 5].

Известно большое количество общедоступных программных средств, предназначенных для восстановления удаленных файлов. Примером может быть утилита Norton Unerase и др. [1, 8]. Можно получить доступ к удаленной информации путем чтения содержимого секторов НЖМД и поиска определенных подстрок. В ходе штатной работы файловой системы процесс перезаписи секторов удаленных файлов требует некоторого периода времени, длительность которого случайна.

В этих условиях нарушитель, имеющий ряд целей по доступу к информации [9] может получить доступ к накопителю с удаленными данными пользователей. Возможны несколько вариантов получения такого доступа. Первый вариант связан с быстрым увеличением объёмов обрабатываемых информационных потоков, совершенствованием ин-

формационных технологий, что определяет необходимость частой замены элементов аппаратной части информационных систем. Устаревшие ПЭВМ утилизируются вместе с данными. Другой вариант доступа к накопителям с информацией представляется процедура реализации ремонта производителем неисправного НЖМД, когда он с удаленной закрытой информацией попадает к неизвестным лицам. А в гарантийный период накопители могут быть заменены (отремонтированы) производителями при условии сохранности пломб и отсутствия механических повреждений, что не позволяет надежно удалить критичную информацию. В качестве третьего варианта выступает вынос оборудования с накопителем (или только самого накопителя) из контролируемого помещения в случае воровства, замены, подмена, дарения и др. Возможны и другие варианты доступа к накопителю конфиденциальной информацией посторонних лиц, в числе которых может быть нарушитель [7, 10].

Известны методы уничтожения информации [1–5, 7, 10], хранимой на НЖМД. Первая группа это аппаратные методы, которые выводят носитель из строя путем его уничтожения. Применение аппаратных методов не всегда рационально и экономически оправдано.

Вторая группа методов это программные методы, которые многократно перезаписывают сектора с удаленными данными псевдослучайной последовательностью и таким образом маскируют защищаемую информацию. Существенные недостатки программных методов заключаются в их низкой надежности и невысоком быстродействии. Проведенные исследования [3–5, 10] показали, что в ходе подобной перезаписи поверх удаляемой информации маскирующей последовательности символов на крайних областях магнитных дорожек жесткого диска остаются поверхности некоторой намагниченности, содержащие информацию о удаленной записи. Нарушитель может провести исследование с помощью специальных устройств магнитный рельеф поверхности пластины жесткого диска для восстановления удаленных данных путем перезаписи другой информации. Известен инструментарий, позволяющий обеспечивать контроль параметров и диагностику рабочих поверхностей НЖМД [11, 12].

Вышесказанное актуализирует разработку адекватной модели канала несанкционированного восстановления конфиденциальной информации, объективно учитывающей условия получения НСД нарушителем для синтеза эффективных методов защиты закрытых данных циркулирующих в современных информационных системах.

Технология магнитной сканирующей микроскопии

Реализация программных методов уничтожения критичной информации, хранимой на магнитных носителях ПЭВМ выполняется путем перезаписи сверху удаляемой информации другой маскирующей последовательности [3–5, 7]. Метод не надежен, т. к. траектория движения головки записи жесткого диска не совпадает полностью с магнитной дорожкой [4, 12–14]. По краям дорожек формируются области остаточной намагниченности, несущие информацию о предыдущих записях.

В целях исследования гарантированности функционирования методов уничтожения информации предполагается, что нарушитель владеет одной из совершенных технологий восстановления информации с высоким разрешением исследования областей намагниченности. Выбор технологии зависит от соотношения достижимой плотности магнитной записи с разрешающей способностью известных технологий восстановления информации.

Производство внешних и внутренних магнитных накопителей отличается постоянным увеличением плотности записи [15–17]. Требуется учитывать это обстоятельство. Этому отвечает метод визуализации магнитных полей [11, 13, 14]. Восстановление удаленных данных возможно в условиях, когда разрешающая способность метода сопоставима с размерами областей остаточной намагниченности [17, 18]. Анализ показывает, что требованию соответствует известный метод магнитной сканирующей микроскопии (МСМ), который характеризуется регулярным увеличением оценок разрешающей способности. Аппаратной частью предложенного метода выступают магнитные силовые микроскопы [12–14]. В основе работы современных сканирующих микроскопов заложены схожие принципы, а их конструкции мало различаются между собой [12–14]. Рассмотрим технологию сканирующей микроскопии более детально. На рис. 1 изображена обобщенная схема сканирующего зондового микроскопа.

С помощью системы грубого позиционирования зонд подводится к поверхности исследуемого образца. При сближении образца и зонда на определенное расстояние, последний начинает взаимодействовать с поверхностными структурами анализируемой поверхности. Расстояние определяется типом исследуемого взаимодействия. Перемещение зонда вдоль поверхности образца осуществляется с помощью сканирующего устройства. Обычно оно представляет собой трубку из пьезокерамики, на поверхность которой нанесены три пары разделенных электродов. Под действием приложенных к пьезотрубке напряжений Ux и Uy она изгибается, обеспечивая тем самым перемещение зонда относительно образца по осям X и Y, под действием напряжения Uz — сжимается или растягивается, что позволяет изменять расстояние игла — образец.

Датчик положения зонда непрерывно отслеживает его позицию относительно образца и через систему обратной связи передает данные о ней в компьютер, управляющий движением сканера. В большинстве сканирующих микроскопов используется оптический датчик. Он регистрирует

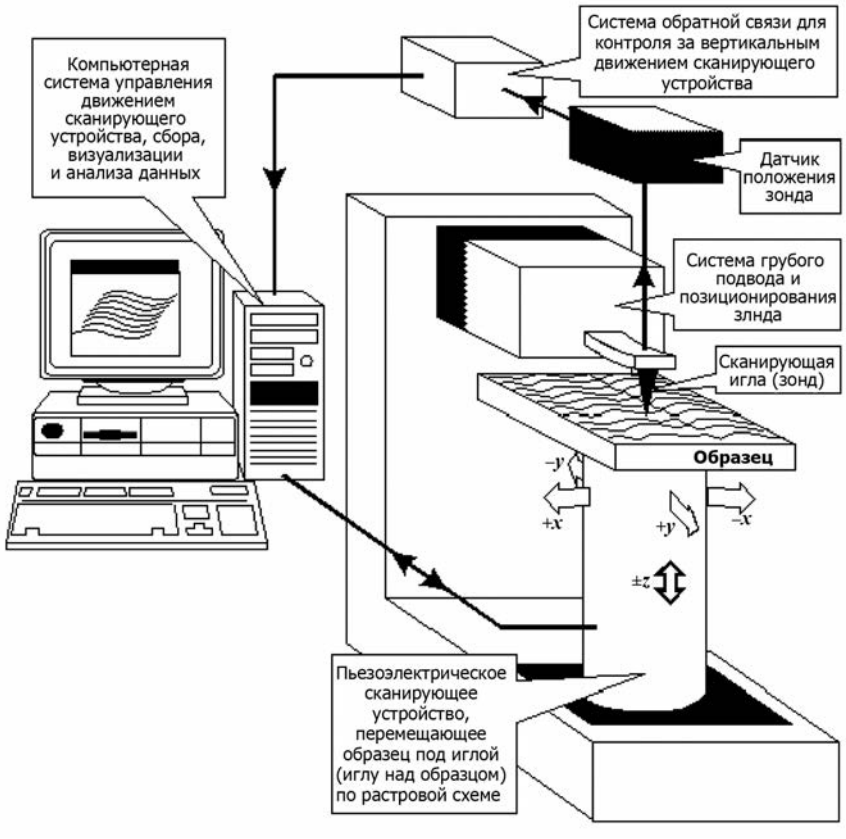


Рис. 1. Обобщенная структурная схема сканирующего зондового микроскопа

угловые перемещения светового луча, отраженного от поверхности кантилевера — упругой микроконсоли зонда. Лазерный луч фокусируется на отражающую поверхность свободного (незакрепленного) конца кантилевера, а измененное положение отраженного луча, свидетельствующее об изгибе кантилевера, определяется с помощью двухсекционного фотодетектора по разностной схеме.

В основе магнитной силовой микроскопии лежит дальнодействующее (10–50 нм) взаимодействие магнитного зонда с локальным магнитным полем образца [13, 14]. Изображение формируется при сканировании зондом исследуемой поверхности и одновременном измерении силы магнитного взаимодействия как функции положения зонда.

Изображение, принимаемое зондом, содержит информацию как о топографии, так и о магнитных свойствах поверхности. Какой из эффектов будет доминировать, зависит от расстояния от зонда до поверхности. Если зонд располагается близко к поверхности, будет преобладать изображение топографии. При увеличении расстояния отображаются магнитные свойства образца. Поэтому регистрацию намагниченности образца обычно проводят с использованием двухпроходной методики [15, 16]. Суть этой методики заключается в том, что зонд проходит над одним и тем же участком дважды: во время первого прохода происходит касание с поверхностью, профиль которой запоминается, а во время второго прохода зонд, поднявшись на заданную высоту, движется по запомненной траектории, реагируя уже только на магнитное взаимодействие. Получаемый от зонда сигнал будет соответствовать карте сил его магнитного взаимодействия с поверхностными структурами образца. При работе по такой методике можно получать одновременно и топографию участка поверхности исследуемого образца, и магнитный образ того же участка.

На рис. 2 показан участок поверхности диска, визуализированный магнитным силовым микроскопом. Детальное рассмотрение показывает, что по краям дорожки заметны граничные области намагниченности, оставленные от предыдущих записей.

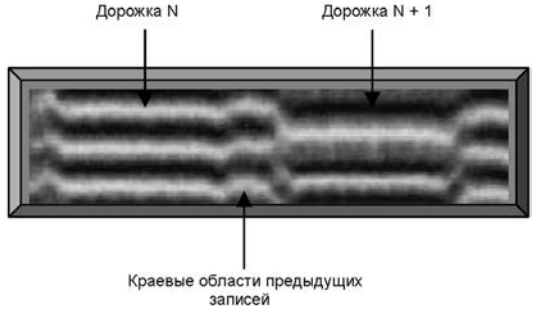


Рис. 2. Визуализация области магнитной поверхности диска

После исследования поверхности диска НЖМД можно восстановить перезаписанные данные из зон остаточной намагниченности.

Выбранная технология является наиболее совершенной для исследования эффектов магнетизма, но применение ее для восстановления перезаписанных данных с НЖМД осложняется некоторыми проблемными ситуациями.

Стоимость МСМ высока. Скорость сканирования метода МСМ невелика [11–13, 17]. В ходе работы микроскопа могут быть получены большие множества изображений магнитной поверхности. Эти изображения необходимо систематизировать для формирования всей картины. Затем необходимо выделить краевые области дорожек, оставшиеся от искомой записи. Данные представляют собой последовательность изменения знаков намагниченности. Моделируется алгоритм считывания информации накопителя в целях получения исходные байт данных исследуемого сектора. Необходимо выполнить еще ряд сложных операций [12, 13] (синхронизация по индексной метке, частичное распознавание для селекции шумов, многократные перекодировки данных). Вышеописанные операции и алгоритмы не публикуются компаниями- производителями и совершенствуются от модели к модели. Отношение сигнал-шум [19] для нормальной работы в считывающей головке значительно выше, чем при моделировании считывания областей остаточной намагниченности. Загрузить полную картину распределения областей остаточной намагниченности в чип канала чтения диска достаточно трудно как программными методами, так и аппаратными.

Размер областей намагниченности случайным образом соотносится с предельным значением разрешающей способности микроскопа, поэтому изображения областей представляют собой запись полезного сигнала с шумом. Имеется вероятность события, что некоторые (случайные) блоки информации восстанавливаемой записи будут декодированы (детектированы) не корректно [20]. Основной причиной ошибок распознавания является дрожание головки НЖМД во время записи имеющее случайную природу. Ошибкой интерпретируется событие, когда след предыдущей записи полностью закрыт текущей записью, или, в случае, когда размер области невелик, и ее комбинация с ранними записями приводит к ошибочному детектированию.

Технология МСМ имеет ряд недостатков, затрудняющих ее использование нарушителем для восстановления информации, однако современная тенденция возрастания плотности записи информации в современных магнитных носителях и увеличивающаяся разрешавшая способность технологии будет еще длительное время определять ее использование в данный момент и в ближайшей и последующей перспективе [3, 4, 14, 19, 21].

Модель канала несанкционированного восстановления информации

Проведенный анализ технологии МСМ позволяет синтезировать модель канала несанкционированного восстановления информации. Объектом несанкционированного доступа для нарушителя является удаленная информация с НЖМД, поверх которой программным методом удаления информации многократно (однократно) записана некоторая зашумляющая (маскирующая) последовательность данных [3, 4, 8].

В качестве *допущений* модели рассматривается следующее:

– для восстановления информации нарушитель использует МСМ оборудование с предельно возможной разрешающей способностью, равной единице измерения информации одному биту [22];

– нарушителю известно полное описание алгоритмов преобразования последовательности знаков смены намагниченности контроллера НЖМД при декодировании полезного сигнала;

– нарушитель имеет возможности составить из отдельных изображений, полученных от МСМ, полное изображение магнитных дорожек НЖМД и выполнить считывание данных из областей остаточной намагниченности любой магнитной дорожки накопителя;

– нарушитель использует информационную избыточность [19, 22] для детектирования записи с ошибками;

– нарушитель точно знает расположение областей восстанавливаемых данных на поверхностях диска и обладает временем, достаточным для многократного (однократного) сканирования участков поверхности магнитного диска.

Ограничениями модели выступает множество адекватных предположений. Первое о том, что при восстановлении с помощью МСМ перезаписанных данных для НЖМД числовое значение вероятности битовой ошибки восстановления перезаписанной информации [20] больше нуля. По мнению специалистов, ее оценка составляет числовую величину порядка 0,65 [11, 13, 14, 21]. Второе предположение связано с тем, что нарушитель не способен оценить абсолютно все множество факторов, влияющих на траекторию движения головки во время записи, маскирующей (зашумляющей) последовательности. Среди основных элементов множества факторов причин возникновения ошибок позиционирования записывающей головки отмечаются следующие:

– турбулентные завихрения потоков воздуха при движении головки над поверхностью диска;

– скрытые производственные дефекты и износ подшипника шпинделя, вала поворотного двигателя блока головок

– погрешности центровки дисков, приводящие во время их вращения к разбалансировке массы диска и биениям;

– непредсказуемая деформация различных частей накопителя из-за нагрева работающего устройства;

– формирование помех в цепи питания от другого оборудования информационной системы [14];

– случайные внешние ударные воздействия, вибрации;

– неточность записи данных при производстве накопителей связанные с случайные дрожания записывающей головки и пластины диска, возникновение электронных шумов и др.

Эти обстоятельства не позволяют ему точно выделить ошибочно детектированный битовый интервал записи.

Третье предположение заключается в том, что каждый блок информации считывается независимо [20, 22] других сканирований, причем повторные считывания блока не увеличивают информацию нарушителя о восстанавливаемой записи накопителя.

Модель канала несанкционированного восстановления информации включает в себя источник информации, представляющий собой поверхность НЖМД и оборудование нарушителя для получения доступа к остаточной информации после ее удаления с диска. Источник с нарушителем связывает канал передачи информации (связи). Нарушитель считывает (восстанавливает) последовательность данных длиной N информационных символов. Канал считывания (передачи) информации от накопителя к нарушителю представляет собой канал НСД (КНСД). Ввиду того, что длина блока равна одному биту и каждый блок считывается независимо от других блоков, сделано предположение о том, что канал восстановления информации нарушителя описывается моделью двоичного симметричного канала связи без памяти [19] с вероятностью битовой ошибки p, причем $p > 0$.

Нарушитель имеет возможность повторить считывание (прием) любого блока сообщения произвольное количество раз, причем в каждом случае он получит одинаковую для всех считываний искаженную версию сообщения, представляющую собой последовательность X^N длиной N бит. В выражении (1) определятся $P_{\text{од}}$ — вероятность ошибочного декодирования (считывания) последовательности X^N:

$$P_{\text{од}} = 1 - (1 - p)^N. \quad (1)$$

Анализ (1) показывает, что $P_{\text{од}}$ определяет вероятность события, при котором случайно порождается хотя бы одна ошибка в процессе формирования сообщения X^N. Среднее число ошибок m в X^N при равномерном распределении [19] можно рассчитать по формуле:

$$M = Np. \quad (2)$$

Величина m в (2) определяется в соответствии с биномиальным законом распределения вероятностей [20] в модели канала несанкционированного восстановления информации.

Заключение

В результате проведенных исследований с учетом адекватной оценки условий НСД нарушителя выбрана рациональная по критерию максимальной разрешающей способности современная технология доступа к удаленной (перезаписанной) информации на НЖМД, которая называется магнитной сканирующей микроскопией. Использование ее нарушителем создает предпосылки для успешного НСД к защищаемой информации, подлежащей удалению с магнитных накопителей [2, 3]. Исследования технологии МСМ показали, что задача восстановления перезаписанной информации является достаточно сложной с отличной от нуля вероятностью ошибочного считывания (детектирования) конфиденциальных данных.

Разработана модель канала несанкционированного восстановления информации описывающая модель нарушителя, условия ведения условия НСД к критичной информации, модель канала считывания информации в рамках адекватных допущений и ограничений. Особенности процесса восстановления информации, выбранный минимально возможный размер блока данных, независимость его считывания и ненулевая вероятность ошибочного детектирования процедур технологии МСМ предопределили описание предлагаемого канала несанкционированного восстановления информации моделью двоичного симметричного канала без памяти [22].

Предлагаемая модель может быть рекомендована специалистам в области построения подсистем защиты информации от несанкционированного доступа современных информационных систем для синтеза адекватной модели нарушителя, разработки и селекции методов защиты, а также оценки надежности предлагаемых методов уничтожения конфиденциальной информации.

Литература

1. *Запечников, С.В., Милославская Н.Г.* Информационная безопасность открытых систем. В 2-х т. Т. 1: Угрозы, уязвимости, атаки и подходы к защите. М.: ГЛТ, 2017. 536 с.

2. *Масалков А.С.* Особенности киберпреступлений в России: инструменты нападения и защита информации. М.: ДМК Пресс, 2018. 226 с.

3. *Белоус А.И., Солодуха В.А.* Кибероружие и кибербезопасность. О сложных вещах простыми словами. М.: Вологда: Инфра-Инженерия, 2020. 692 с.

4. *Zhang Q., Jia S., Chang B., Chen B.* Ensuring data confidentiality via plausibly deniable encryption and secure deletion — a survey // Cybersecurity. 2018. No. 1(1). Doi: 10.1186/s42400–018–0005–8

5. *Жилина А.А.* Методы уничтожения данных с жесткого диска // Научные записки молодых исследователей. 2020 № 8(4). С. 65–73.

6. *Спесивцев А.В., Вегнер В.А., Крутяков А.Ю.* Защита информации в персональных ЭВМ. М.: Радио и связь, 2016. 192 с.

7. *Cai Y., Ghose S., Haratsch E.F., Luo Y., Mutlu O.* Reliability Issues in Flash-Memory-Based Solid-State Drives: Experimental Analysis, Mitigation, Recovery // Inside Solid State Drives (SSDs). Springer Series in Advanced Microelectronics. By. eds. Micheloni R., Marelli A., Eshghi K. 2018. Vol. 37. Springer, Singapore. Doi: 10.1007/978–981–13–0599–3_9

8. *Чипига, А.Ф.* Информационная безопасность автоматизированных систем. М.: Гелиос АРВ, 2017. 336 с.

9. Патент РФ RU2613845. Способ шифрования/дешифрования / Деньжонков К.А., Остроумов О.А., Синюк А.Д., Филимонов В.А., Савищенко Н.В. Заявл. 01.04.2016. Опубл. 21.03.2017. Бил. № 9.

10. *Song K.M., Jeong J.-S., Pan B., Zhang X., Xia J., Cha S., Park T.-E., Kim K., Finizio S., Raabe J., Chang J., Zhou Y., Zhao W., Kang W., Ju H., Woo S.* Skyrmionbased artificial synapses for neuromorphic computing // Nature Electronic. 2020. No. 3. Pp. 148–155.

11. *Woo S., Litzius K., Kr¨uger B., Mi-Young Im, Caretta L., Richter K., Mann M., Krone A., Reeve R. M., Weigand M., Agrawal P., Lemesh I., Mawass M.-A., Fischer P., Kläui M., Beach G. S. D.* Observation of room-temperature magnetic skyrmions and their current-driven dynamics in ultrathin metallic ferromagnets // Nature Mater. 2016. No. 15. Pp. 501–506.

12. *Бизяев Д.А., Бухараев А.А., Бедин С.А., Загорский Д.Л., Долуденко И.М.* Магнитно-силовая микроскопия в исследовании металлических нанопроволок, полученных репликацией пор в трековой полимерной матрице // Материалы 12-й международной конференции «Взаимодействие излучений с твердым телом» (Минск, Беларусь, 19–22 сентября 2017. Минск: Изд. центр БГУ, 2017. С. 309–311.

13. *Филонов А.С., Яминский И.В.* Организация Интернет–лаборатории сканирующей зондовой микроскопии на базе комплекса ФемтоСкан Онлайн. URL: http://www.nanoscopy.net (дата обращения 7.11.2018).

14. *Еременко В.Г.* Влияние ориентации магнитного момента зонда магнитно-резонансного силового микроскопа на спектры спин-волновых резонансов // XXVII Российская конференция «Современные методы электронной и зондовой микроскопии в исследованиях органических, неорганических наноструктур и нано-биоматериалов». (Черноголовка, 28–30 августа 2018). Черноголовка, 2018. С. 131–133.

15. *Coughlin T.M.* Fundamentals of Hard Disk Drives. In: Digital Storage in Consumer Electronics. Springer, Cham. 2018. Pp. 25–44. Doi: 10.1007/978–3–319–69907–3_2

16. *Rombach P., Keuper J.* SmartPred: Unsupervised Hard Disk Failure Detection // High Performance Computing. ISC High Performance 2020. Lecture Notes in Computer Science. By eds. Jagode H., Anzt H., Juckeland G., Ltaief H. 2020. Vol. 12321. Springer, Cham. Doi: 10.1007/978–3–030–59851–8_15

17. *Soumyanarayanan A., Raju M., Gonzalez Oyarce A. L., Tan A. K. C., Mi-Young Im, Petrović A. P., Pin Ho, Khoo K. H., Tran M., Gan C. K., Ernult F., Panagopoulos C.* Tunable room-temperature magnetic skyrmions in Ir/Fe/Co/Pt multilayers // Nature Mater. 2017. No. 16. Pp. 898–904.

18. *Maccariello D., Legrand W., Reyren N., Garcia K., Bouzehouane K., Collin S., Cros V., Fert A.* Electrical detection of single magnetic skyrmions in metallic multilayers at room temperature // Nature Nanotech. 2018. No. 13. Pp. 233–237.

19. *Синюк А.Д., Остроумов О.А.* Постановка задачи кодирования общей информации широковещательного канала // Вестник компьютерных и информационных технологий. 2017. № 1. С. 16-20. Doi: 10.14489/vkit.2017.01.pp.016–020

20. *Сысуев С.Ю., Остроумов О.А., Синюк А.Д.* Теорема о максимальной вероятности ошибки кода в дискретном широковещательном канале связи // Информация и космос. 2019. № 3. С. 54–59.

21. *Uzdin M., Potkina M.N., Lobanov I.S., Bessarab P.F., J´onsson H.* Energy surface and lifetime of magnetic skyrmions // J. Magn. Magn. Mater. 2018. No. 459. Pp. 236–240.

22. *Остроумов О.А., Синюк А.Д.* Исследование совместной информации // Информация и космос. 2017. № 3. С. 55–58.

UNAUTHORIZED INFORMATION RECOVERY CHANNEL MODEL

ALEXANDER D. SINYUK
St.Petersburg, Russia, eentrop@rambler.ru

OLEG A. OSTROUMOV
St. Petersburg, Russia, oleg-26stav@mail.ru

KEYWORDS: hard disk drives; confidential information deletion; residual magnetization areas; intruder; magnetic force microscopy; channel for unauthorized information recovery; model of binary symmetric channel without memory.

ABSTRACT

Large amounts of information are stored in hard disk drives. In modern information systems. Deleting files using the operating system or reformatting the magnetic drive does not delete the data. There is an opportunity to recover the data by the violator in the conditions of moving the drive from the controlled premises for disposal, sending for repair, theft, replacement, substitution, donation, etc. The known information destruction methods are not always economical and do not fully meet the reliability requirement. The modern methods selection of information recovery is carried out. During the implementation of software methods for destroying information, the overwriting of the masking sequence above deleted information is carried out. This does not guarantee its destruction, because the motion path of the hard disk recording head does not exactly coincide with the magnetic track, and residual magnetization regions carrying information about previous records are formed at the edges. It is assumed that the intruder owns one of the most advanced high-resolution information recovery technologies for studying the areas of residual magnetization. The technology of magnetic scanning microscopy is proposed, which is closely associated with an increase in the recording density of information on storage devices. The carried out operating principles analysis of modern magnetic scanning microscopes made it possible to create conditions for the model development of an unauthorized information recovery channel that includes an information source representing the drive

surface and the intruder's equipment for access to residual information. A source with an intruder connects an information transmission channel, which is proposed to be described by a model of a binary symmetric channel without memory. The erroneous recovery probability estimates of deleted information block and the errors average number in an information block are given. The results can be recommended to specialists in the field of building subsystems to protect information from unauthorized access to information systems for the synthesis of an adequate model of the intruder, development and selection, as well as assessing the developed methods reliability for the confidential information destruction.

REFERENCES

1. Zapechnikov S.V., Miloslavskaya N.G. *Informationay bezepasnost' otkritih system. Tom 1: Ugrozy, uyazvimosti, ataki i podhody k zaschite* [Open systems information security. In 2 vol. Vol.1: Threats, vulnerabilities, attacks and approaches to protection]. Moscow: GLT, 2017. 536 p. (In Rus)
2. Masalkov A.S. *Osobennosti kiberprestuplenii v Rossii: instrumenti napadenia I zashita informachii* [Features of cybercrimes in Russia: tools of attack and protection of information].Moscow: DMK Press, 2018. 226 p. (In Rus)
3. Belous A.I., Solodukha V.A. *Kiberorujie i kiberbezopasnost. O slojnix veschax prostimi slovami* [Cyber weapons and cyber security. About complex things in simple words]. Moscow: Vologda: Infra-Engineering, 2020. 692 p. (In Rus)
4. Zhang Q., Jia S., Chang B., Chen B. Ensuring data confidentiality via plausibly deniable encryption and secure deletion – a survey. *Cybersecurity.* 2018. No. 1(1). Doi: : 10.1186/s42400–018–0005–8
5. Zhilina A.A. Hard drive data erasure. *Nauchnye zapiski molodykh issledovatelei* [Scientific notes of young researchers]. 2020. No. 8(4). Pp. 65–73. (In Rus)
6. Spesivtsev A.V., Vegner V.A., Krutyakov A. Yu. *Zashita informachii v personal'nih IBM* [Information protection in personal computers]. Moscow: Radio i svyaz', 2016. 192 p. (In Rus)
7. Cai Y., Ghose S., Haratsch E.F., Luo Y., Mutlu O. Reliability Issues in Flash-Memory-Based Solid-State Drives: Experimental Analysis, Mitigation, Recovery. In: Micheloni R., Marelli A., Eshghi K. (eds). I*nside Solid State Drives (SSDs). Springer Series in Advanced Microelectronics.* 2018. Vol 37. Springer, Singapore. Doi: 10.1007/978–981–13–0599–3_9
8. Chipiga A.F. *Informationay bezopasnost' avtomatizirovannih system* [Automatic systems Information security]. Moscow: Gelios, 2017. 336 p. (In Rus)
9. Patent RF 2613845. Sposob shifrovania / deshifrovania [Method of encryption / decryption]. Denzhonkov K.A., Ostroumov O.A., Sinyuk A.D., Filimonov V.A., Savishchenko N.V. Declared 01.04.2016. Published 21.03.2017. Bulletin No. 9. (In Rus)
10. Song K.M., Jeong J.-S., Pan B., Zhang X., Xia J., Cha S., Park T.-E., Kim K., Finizio S., Raabe J., Chang J. , Zhou Y., Zhao W., Kang W., Ju H., Woo S. Skyrmionbased artificial synapses for neuromorphic computing. *Nature Electronic.* 2020. No. 3. Pp. 148–155.
11. Woo S., Litzius K., Kr ̈uger B., Mi-Young Im, Caretta L., Richter K., Mann M., Krone A., Reeve R. M., Weigand M., Agrawal P., Lemesh I., Mawass M.-A., Fischer P., Kläui M., Beach G. S. D. Observation of room-temperature magnetic skyrmions and their current-driven dynamics in ultrathin metallic ferromagnets. *Nature Mater*. 2016. No. 15. Pp. 501–506.
12. Bizyaev D.A., Byharev A.A, Bedin C.A., Zagorskii D.L., Doludenko I.V. Magnitno-silovaya mikroskopia v issledovanii metalicheskix nanoprovolok, poluchennix replikaciei por v trekovoi polimernoi matrice [Magnetic force microscopy in the study of metal nanowires obtained by pore replication in a track polymer matrix]. *Materialy 12 mejdunarodnoi konferencii "Vzaimodeistvie izlucenii s tvedim telom"* [Materials of the 12th international conference "Interaction of radiation with a solid", Minsk, Belarus 19–22 September 2017]. Minsk: Izdatel'skii chenter BGU [Publication center BGU], 2017. Pp. 309–311. (In Rus)
13. Filonov A.S., Yaminsky I.V. *Organizaciya internet laboratorii skaniruushei zondovoi mikroskopii na base kompleksa FemtoScan onlain* [The scanning probe microscopy internet laboratory organization based on FemtoScan complex Online]. URL: http://www.nanoscopy.net (date of access 7.11.2018). (In Rus)
14. Eremenko V.G. Vliyaniye oriyentatsii magnitnogo momenta zonda magnitno-rezonansnogo silovogo mikroskopa na spektry spin-volnovykh rezonansov [Influence of the orientation of the magnetic moment of the probe of a magnetic resonance force microscope on the spectra of spin-wave resonances]. *XXVII Rossiyskaya konferentsiya "Sovremennyye metody elektronnoy i zondovoy mikroskopii v issledovaniyakh organicheskikh, neorganicheskikh nanostruktur i nano- biomaterialov"* [XXVII Russian conference "Modern methods of electron and probe microscopy in the study of organic, inorganic nanostructures and nano-biomaterials", Chernogolovka, August 28–30, 2018]. Chernogolovka, 2018. Pp. 131–133. (In Rus)
15. Coughlin T.M. *Fundamentals of Hard Disk Drives.* In: Digital Storage in Consumer Electronics. Springer, Cham. 2018. Doi: 10.1007/978–3–319–69907–3_2
16. Rombach P., Keuper J. SmartPred: Unsupervised Hard Disk Failure Detection. In: Jagode H., Anzt H., Juckeland G., Ltaief H. (eds). *High Performance Computing. ISC High Performance 2020.* Lecture Notes in Computer Science, vol 12321. Springer, Cham. DOI: 10.1007/978–3–030–59851–8_15
17. Soumyanarayanan A., Raju M., Gonzalez Oyarce A. L., Anthony K. C. Tan, Mi-Young Im, Petrović A. P., Pin Ho, Khoo K. H., Tran M., Gan C. K., Ernult F., Panagopoulos C. Tunable room-temperature magnetic skyrmions in Ir/Fe/Co/Pt multilayers. *Nature Mater*. 2017. No. 16. Pp. 898–904.
18. Maccariello D., Legrand W., Reyren N., Garcia K., Bouzehouane K., Collin S., Cros V., Fert A. Electrical detection of single magnetic skyrmions in metallic multilayers at room temperature. *Nature Nanotech*. 2018. No. 13. Pp. 233–237.
19. Sinyuk A.D., Ostroumov O.A. The task setting of broadcast communication channel general in formation coding. *Vestnik komp'iuternykh i informatsionnykh tekhnologii* [Herald of computer and information technologies]. 2017. No. 1. Pp. 16-20. Doi: 10.14489/vkit.2017.01.pp.016–020 (In Rus)
20. Sysuev S. Yu., Sinyuk A.D., Ostroumov O.A. Theorem about the maximum probability of a code error in a discrete broadcast communication channel. *Informatsiya i kosmos* [Information and space]. 2019. No. 3. Pp. 54–59. (In Rus)
21. Uzdin M., Potkina M.N., Lobanov I.S., Bessarab P.F., J´onsson H. Energy surface and lifetime of magnetic skyrmions. *J. Magn. Magn*. Mater. 2018. No. 459. Pp. 236–240.
22. Ostroumov O.A., Sinyuk A.D. Issledovaniye sovmestnoy informatsii [Joint information research]. *Informatia i kosmos* [Information and space]. 2017. No. 3. Pp. 55–58. (In Rus)

INFORMATION ABOUT AUTHORS:

Sinyuk A.D., PhD, Docent, Professor of the Telecommunication military academy;
Ostroumov O.A., PhD, Doctoral candidate of the Telecommunication military academy.

For citation: Sinyuk A.D., Ostroumov O.A. Unauthorized information recovery channel model. *H&ES Research*. 2021. Vol. 13. No. 3. Pp. 60–67. Doi: 10.36724/2409-5419-2021-13-3-60-67 (In Rus)

Doi: 10.36724/2409-5419-2021-13-3-68-75

КРИПТОГРАФИЧЕСКАЯ КОНТЕЙНЕРИЗАЦИЯ ДАННЫХ В ОБРАБОТКЕ НЕЙРОННЫХ СЕТЕЙ ГЛУБОКОГО ОБУЧЕНИЯ

ТЮТЮННИК
Александр Анатольевич[1]

ЛАЗАРЕВ
Алексей Игоревич[2]

АННОТАЦИЯ

Введение: существующее развитие методов обеспечения информационной безопасности в сфере информационных технологий позволяет контролировать конфиденциальность данных лиц на вариативных уровнях. Аппаратными решениями могут являться портативные криптографические ключи, а также узконаправленные устройства биометрической идентификации личности. Программными решениями являются методы статической проверки при помощи последовательностей и побочные средства развертки систем виртуализации данных. Основная проблема, выделяемая среди вышеописанных методов – необходимость в наличии дополнительных аппаратных средств, выступающих токенами, инфракрасными камерами, датчиками биометрической идентификации. Альтернативной проблемой является недостаточная защищённость программных решений, так как наличие уязвимостей нулевого дня позволяет снизить безопасность, что приводит к возможности перехвата конфиденциальных данных третьим лицами.**Цель исследования:** выражается в анализе и разработке программных методов и алгоритмов обеспечения безопасности данных на основе методов контейнеризации. Разработанное программное решение позволяет осуществлять выполнение прикладных задач в защищённом контейнере, при этом реализованные методы аутентификации поддерживают возможность идентификации личности как при помощи последовательностей, так и с использованием прикладного программного интерфейса Windows Hello. **Используемые методы:** методы и алгоритмы обеспечения безопасности, направленные на реализацию уникального криптографического алгоритма. **Результаты** исследованных методов и алгоритмов развёртки ограниченной оболочки позволяют вариативно подбирать оптимальные исходы работы внутренних экземпляров процессов наряду с реализацией криптографических методов. Прикладное программное обеспечение основано на совместном использовании средств виртуализации и методов взаимодействия посредством нейросетевых технологий. Обособленность данного решения от альтернативных методов заключается в возможности применения контейнера без значительных затрат аппаратных ресурсов и отсутствия первичных знаний в настройке программного модуля. **Практическая значимость** заключается в возможности использования методов и алгоритмов при построении защищенных рабочих мест в организациях малого и среднего бизнеса.

КЛЮЧЕВЫЕ СЛОВА: криптозащита; контейнеризация; нейронная сеть; глубокое обучение; идентификация личности.

Сведения об авторах:

[1]к.э.н., доцент, преподаватель филиала Национального исследовательского университета «Московский энергетический институт» в г. Смоленске, г. Смоленск, Россия, tyutyunnik.aa@yandex.ru

[2]студент филиала Национального исследовательского университета «Московский энергетический институт» в г. Смоленске, г. Смоленск, Россия, anonymous.prodject@gmail.com

Для цитирования: *Тютюнник А.А., Лазарев А.И.* Криптографическая контейнеризация данных в обработке нейронных сетей глубокого обучения // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13. № 3. С. 68–75. Doi: 10.36724/2409-5419-2021-13-3-68-75

Введение

Обеспечение безопасности пользователей персональных компьютеров является приоритетной задачей разработчиков системного и прикладного программного обеспечения (ПО). Правильно выполненная конфигурация персонального компьютера позволяет в дальнейшем выпускать кумулятивные обновления ПО для исправления возможных уязвимостей, позволяющих третьим лицам получить несанкционированный доступ к целевой системе [1]. Основной приоритет безопасности, выделяемый на примере операционной системы (ОС) Microsoft Windows 10 компании Microsoft, реализуется за счёт использования средств защитника Windows Security для частных лиц и иерархической системы безопасности, учёта и контроля пользователей домена для корпоративных клиентов, использующих ОС Microsoft Windows Server 2019 [2]. Применение описываемых средств явно повышает уровень безопасности, однако для тестирования и отладки программного обеспечения на данный момент целесообразным является интеграция решений на базе технологий виртуализации как от компании Microsoft — Windows Sandbox или Hyper-V, так и сторонних разработчиков, например, компании VMWare, выпускающей такие продукты как Workstation PRO, vSphere и множество других [3–4]. Приоритетная проблема, выделяемая в данном случае, заключается в том, что средства виртуализации и контейнеризации в большей степени требуют значительных затрат физических ресурсов операционной системы, при этом решение от компании Microsoft не имеет встроенных средств обеспечения безопасности конфиденциальных данных. В альтернативном варианте сторонние решения, предоставляющие как обширные функциональные возможности, так и возможность обеспечения безопасности, предполагаются для использования только в организациях с лицензированием по подписке. Таким образом можно сделать вывод, что на данный момент не существует прикладных решений, предоставляющих гибкую и малотребовательную технологию виртуализации прикладного ПО для частных клиентов, позволяющую осуществлять запуск, тестирование и отладку прикладного ПО в безопасной среде, что делает данную проблему актуальной на момент реализации программного продукта.

В качестве решения данной проблемы было разработано программное обеспечение, позволяющее осуществлять безопасный запуск копии исполняемого файла в ограниченном по ресурсам контейнере. Основная разработка осуществлялась на базе применения средств встроенного компонента виртуализации Windows Sandbox в качестве базового контейнера и дополнительных средств безопасности, осуществляющих интеграцию алгоритма аутентификации в оболочку посредством Application Programming Interface (API) Windows Hello — такое решение было протестировано на совместимом с Windows Hello аппаратном оборудовании, что в результате позволяет осуществлять процесс аутентификации за счёт средств биометрии, представляемыми дактилоскопическими сканерами отпечатков пальцев, модулями инфракрасных IR-камер распознавания лица и множеством других [5]. Для реализации интерактивного взаимодействия с конечным пользователем в разработанное ПО был интегрирован нейронных модуль, базирующийся на основе теорий в области искусственного интеллекта, а в частности — алгоритмов двунаправленной рекуррентной нейронной сети (BRNN), и позволяющий на основе действий пользователя осуществлять предиктивную автоматизацию отдельных процессов.

Обособленность интеграции прикладных средств виртуализации

На первоначальном этапе планирования общего алгоритма работы разработанного ПО были выделены некоторые прикладные средства, предоставляющие пользователю возможность виртуализации программ в специфичном контейнере. Одним из таких компонентов является Microsoft Windows Sandbox, предоставляющий пользователю оболочку на базе изолированной виртуальной машины Hyper-V, и позволяющей запускать Windows приложения в изолированной среде [6]. В качестве системных требований, предъявляемых конечному пользователю, можно выделить необходимость в копии ОС Microsoft Windows 10 редакции Pro, совместимой архитектуры x86_x64, поддержки виртуализации на аппаратном уровне и 4 ГБ ОЗУ. Как показано на рисунке, виртуальная среда предоставляет собой копию операционной системы разрядности Enterprise, 40 ГБ физического места и предустановленную ОС для исполнения программного обеспечения (рис. 1).

Обособленность выбора программного решения Windows Sandbox представляется скоростью запуска, отсутствием дополнительных расходов со стороны побочных эффектов — затрат на интернет-соединение, поиск специализированного оборудования. Помимо прочего, данный продукт поддерживает взаимодействие с сторонними модулями и возможность настройки параметров работы перед инициализацией. Основной процесс взаимодействия осуществляется на основе выполнения скриптов Power Shell (PS) — на этапе планирования список доступного функционала был расширен до возможности запуска нескольких копий средств виртуализации, контроля параметров использования графического процессора, а также выбора сетевого адаптера, используемого в оболочке [7–8].

На этапе планирования и визуализации иерархической составляющей программногопродукта были выделены составляющие программного обеспечения. В качестве основного языка программирования используется Python совместно с интеграцией скриптов PS [9–10]. На рисунке

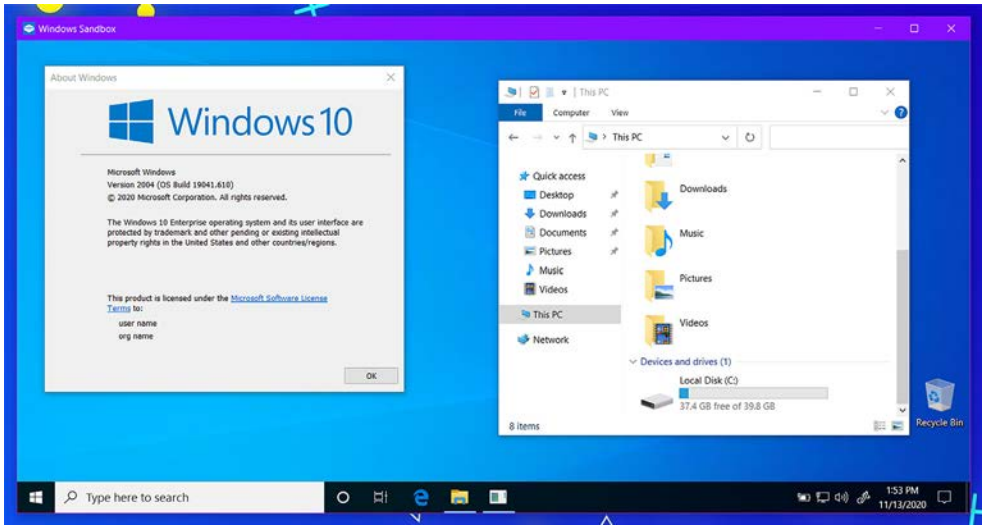


Рис. 1. Виртуализация Windows Sandbox на базе Hyper-V

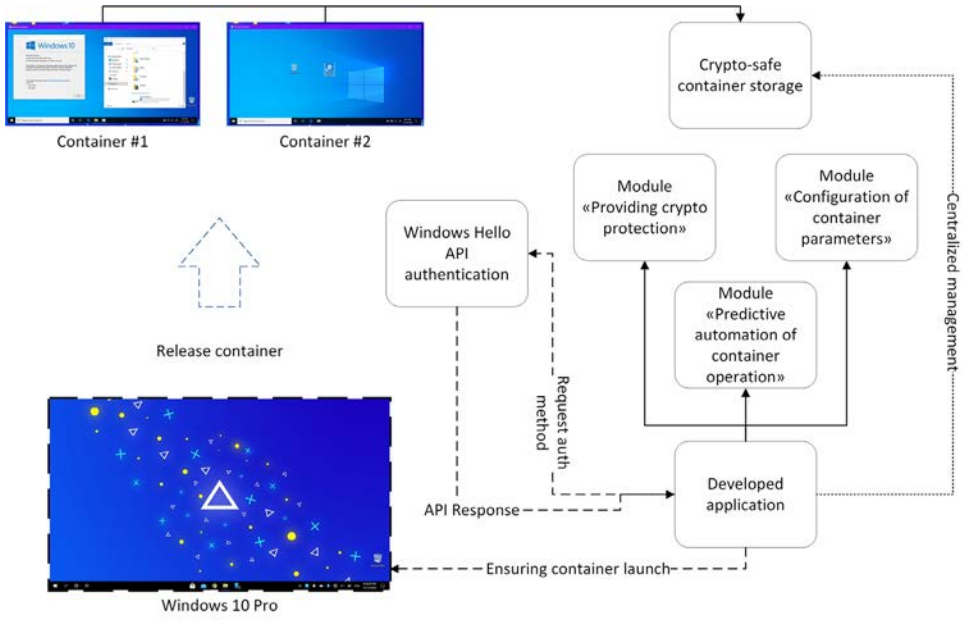


Рис. 2. Общая схема взаимодействия контейнеров и разработанного ПО

представлены основные компоненты и принцип взаимодействия модулей и крипто-контейнера (рис. 2).

– модуль «генерация начальных параметров» используется для задания первоначальных пользовательских настроек — количества контейнеров, способа аутентификации, возможности интеграции дополнительных скриптов автозапуска, выбора выделяемой памяти контейнера и возможности сохранения данных после завершения работы;

– модуль «организация работы криптозащищенного хранилища» предполагает изменение специфичных параметров безопасности контейнера: выбора пути хранения целевого контейнера, а также возможность шифрования и дешифрования контейнера по времени, или дешифрование на время работы экземпляра процесса контейнера с последующим шифрованием после завершения работы;

– модуль «предиктивная автоматизация работы контейнера» использует нейросетевые библиотеки для автоматизации действий пользователя на основе анализа его работы с контейнером. Также пользователю предлагается возможность выбора метода анализа и специфику работы — работа с документами, работа с специализированными программами. Немаловажной является функция повышения безопасности, которая позволяет выполнить

точный анализ и принятие решений, направленная на невозможность утечки персональных данных.

Согласно иллюстрации, схема взаимодействия разработанного ПО осуществляется следующим образом: запущенный экземпляр приложения выполняет запрос в модуль Windows Hello посредством API разработчика, а затем, в случае верного ответа выполняется запуск целевого контейнера в операционной системе [11] (рис. 2). В тоже время дополнительный процесс ПО выполняет расшифровку директории на время активности окна экземпляра контейнера, при этом модуль предиктивной автоматизации осуществляет сканирование всех запущенных процессов в самой системе и соответствующем контейнере с целью выявления алгоритмов работы пользователя.

Метод реализации крипто-защищённого контейнера

Интеграция модифицированных функций в процесс виртуализации осуществляется на основе применения конфигурации во время запуска экземпляра контейнера. Основной синтаксис, используемый в файле конфигурации, соответствует правилам построения xml разметки (рис. 3) [12]. Исходя из представленной иллюстрации можно сказать, что ввиду использования привычных команд для запуска внутренних экземпляров приложения, монтирования директорий, представляется возможным осуществлять редактирование конфигурации при помощи нейронной сети, которая на основе действий пользователя осуществляет изменение конфигурационного файла.

```
<Configuration>
  <VGpu>Enable</VGpu>
  <Networking>Enable</Networking>
  <MappedFolders>
  </MappedFolders>
  <LogonCommand>
  <Command>start "" "C:\Users\WDAGUtilityAccount\Desktop\Documents\vmware.exe" </
Command>
  </LogonCommand>
</Configuration>
```

Рис. 3. Пример конфигурации с запуском виртуальной машины внутри контейнера

Основная директория контейнера представляет собой путь, задаваемый параметром «<SandboxFolder>», другие примечательные ограничения отсутствуют. Существующий метод шифрования рабочего каталога основан на использовании технологии шифрования Encrypted File System (EFS) в котором существенным недостатком можно выделить необходимость в хранении закрытого ключа и сертификата безопасности, а также наличия ОС редакции вида Pro или Enterprise [13]. Ввиду того, что процесс работы с контейнером является автоматизированным, данный метод шифрования не является целесообразным в применении. Для решения этой проблемы был разработан метод шифрования, основанный на параллельном использовании алгоритмов сжатия LZMA2 и функций хеширования MD5 [14–15]. Общий процесс работоспособности криптозащиты реализуется посредством компрессии директории «<SandboxFolder>», при этом основным ключом защиты выступает итоговое значение хэш-функции. Алгоритм генерации хэш-функции основан на использовании переменных нескольких потоков различных источников — идентификатор уникального отпечатка в общей сложности генерируется по формуле 1.

$$HASH\left[FINGERPRINT\right] = DEST\_DIR \rightarrow SESSION\_ID, \quad (1)$$

где FINGERPRINT — функция вызова генерации отпечатка;

DEST_DIR — хэш-значение целевой директории;

SESSION_ID — функция получения уникального хэш-значения текущей сессии ОС Windows 10.

Ввиду того, что представляется возможным использовать крипто-контейнер в различных сессиях, процесс хранения хэш-функций осуществлён при помощи реестра. В качестве основной ветки реестра используется «HKLM\SOFTWARE\CRYPTO-CONTAINER» и соответствующие ключи «DESTINATION_F», «SESSION_ID_F», «FINGERPRINT» строкового типа (string).

Алгоритмическое сжатие LZMA2 выполняется посредством вызова функции компрессии из набора разработчика LZMA Setup Development Kit (SDK), при этом основные параметры сжатия (уровень компрессий, количество потоков) являются динамическими и рассчитываются нейронной сетью на основе текущей загрузки системы — объем доступной памяти, текущая нагрузка центрального и графического процессора [16–17].

В общем случае процесс вызова модулей шифрования и дешифрования основан на отслеживании процессов в текущей сессии Windows по PID и времени запуска процессов. Результатом работы данного модуля обеспечивается функционал шифрования директории с последующей расшифровкой на время работы копии контейнера, при этом процесс шифрования выполняется на основе подбора оптимизированных параметров текущей загрузки системы пользователя.

Предиктивная работа контейнера на основе двунаправленных RNN

Модуль предиктивной автоматизации отдельных процессов основан на интеграции модуля BRNN. Основной принцип работы предиктивного модуля выражается в возможности анализа запущенных процессов как в основной системе, так и в контейнере. Основной возможностью использования BRNN является возможность предиктивного анализа последовательности, выступающей динамическим

параметром системы [18–19]. Управление данным модулем было разделено на несколько отдельных функциональных процессов, предлагающих пользователю различные возможности для анализа и автоматического принятия решений:

– «Минимальное потребление памяти и оптимизация работы в режиме энергосбережения». Выражается в возможности сокращения используемой памяти и оптимизации работы запущенных приложений — предполагается для использования при малом распределении памяти и наличии высоко-потребляемых процессов работы в основной операционной системе. В данном варианте побочные процессы, не используемые по назначению, принудительно завершаются по параметру PID.

– Процесс «Оптимальное потребление ресурсов» нацелен на изменение приоритетов задач, активных в текущий момент времени. Предполагается работа с ресурсоёмким программным обеспечением в одном временном промежутке — например, запуск виртуальной машины на базе ядра Linux в vSphere и тестирование уязвимости в отдельном контейнере.

– Процесс «Режим обеспечения стабильной работы» предполагает использование системных ресурсов с неограниченными физическими процессами. В данном режиме осуществляется анализ ресурсозависимых компонентов и устранение возможности вызова функции отображения ошибки Windows из-за ошибок в различных программных компонентах — переполнения буфера памяти, ошибок в сравнениях сумм.

Процессы нейронной сети представляют иерархическую архитектуру, представляемую модулями анализа доступных ресурсов, процессов и действий пользователя. Модуль анализа доступных ресурсов использует параметры доступного и использованного объема оперативной памяти, места на физическом носителе, а также объем используемой и возможной выделяемой видеопамяти. Реализация BRNN выполняет параллельную обработку экземпляров процессов нейронной сети — входные вектора в первом варианте подаются в стандартном виде рекуррентной нейронной сети, второй вариант предполагает подачу вектора в обратном порядке [20]. Затем выходные вектора объединяются в единичный вектор на каждом шаге времени t, при этом предоставляется возможность получения значения последовательности в различные моменты времени.

В качестве основных параметров, подаваемых на вход нейронной сети, представляются значения фаззификатора в виде векторов x_i, выходным значением для каждого процесса нейросети является вектор z_i (формула 5). С учётом необходимости в обучении рассматриваемой нейронной сети, на вход векторов подаются одномерные массивы, например количество доступной оперативной памяти (x_1) (прим.— 15.800), количество используемой оперативной памяти (x_2) (прим.— 8200), и соответственно количество памяти, необходимой для стабильной отработки внутренних функций системы (x_3) (прим.— 4000). Первичный слой x_1 выступает двунаправленным, и активируется при помощи класса bidirectional. В результате, вектор определения обратного выхода будет иметь значение z_{t-1} на основе формулы 5.

Выходным значением будет является единичное число (вектор z_i), превышение которого вызывает функции принудительного завершения работы отдельных процессов, отключения анимации и других функций ограничения работы системы (формула 5). В качестве функции активации выступают формулы 2–3.

$$o = \sigma(W \bullet [q, x]), \tag{2}$$

где o_t — функция активации первого нейрона;
q — скрытый слой обработки прямого распространения;
x_i — входные параметры нейронной сети;
t — этап состояния рекуррентной функции.

$$r = \sigma(W \bullet [q, x]), \tag{3}$$

где r_t — функция активации функции обратного нейрона;
q — скрытый слой обработки обратного распространения;
x_i — входные параметры нейронной сети;
t — этап состояния рекуррентной функции.

Формула для работы скрытого слоя обратного распространения сети q_i будет следующей (Формула 4):

$$\tilde{q} = \tan q(W * [r * q, t]), \tag{4}$$

где q — слой обработки входных значений (скрытый);
r_t — функция активации;
i — входные параметры нейронной сети;
t — этап состояния рекуррентной функции.

При этом формула, представляющая скрытый слой прямого распространения, будет иметь вид:

$$z = (1 - o) * q + o * \tilde{q}, \tag{5}$$

где z — выходной вектор нейронной сети;
q_t — слой обработки входных значений;
o_t — функция активации;
q — скрытый слой;
t — этап состояния рекуррентной функции.

Программная реализация осуществляется на базе отдельного модуля Python — PyTorch [20]. На этапе инициализации двунаправленного слоя вначале осуществляется подключение GRU слоя (параметр bidirectional), затем выполняется инициализация GRU слоя для вычисления обратной последовательности (параметр bidirectional принимает значение false). На следующем этапе выполняется

проверка сходимости весов обратного и реверсивного двунаправленного слоя нейронных сетей в единичном промежутке времени. В качестве выборки подаваемых данных функции «train_data» рассматривается подача данных PID экземпляров процессов и используемой оперативной памяти с помощью последовательностей типа плавающей точки (float). Вариант реверсивного входа использует функцию «reverse_gru» для подачи значений последовательности массива «train_data».

```
train_data = {
“5.648”, “10.888”: False,
“4.636”, “12.1352”: False,
“13.534”, “14.235”: True,
}
```

На основе функции реверсивного вывода за счёт выходных последовательностей выполняется аналитическое сравнение векторов выходной последовательности и исходной при помощи базы знаний нечетких правил.

Интерполяция целевых значений осуществляется на базе библиотеки FuzzyWuzzy, в частности на основе сравнения значений с использованием функции извлечения (process.extract) и функции проверки токена на сравнение [21]. В случае повышения процентного соотношения осуществляется запуск дополнительных функций в системе, например, при работе ПО в режиме минимального потребления памяти осуществляется запуск процесса принудительного завершения работы экземпляра процесса с наиболее низким приоритетом.

Иначе говоря, реализация ПО в соответствии с интеграцией двунаправленной нейронной сети и базами правил выполняется по алгоритму (рис. 4).

Проиллюстрированный в работе алгоритм взаимодействия сводится к извлечению требуемых динамических параметров системы для дальнейшего представления в качестве входных векторов BRNN (рис. 4). Далее выполняется передача выходных образцов в модуль нечеткой логики FuzzyWuzzy который определяет необходимость завершения работы процессов на основе выбранного режима работы ПО для поддержки стабильной работы контейнера. Параллельно с работой модуля нейронной сети осуществляется фоновое отслеживание экземпляра контейнера — при запуске процесса выполняется дешифрование, а затем выполняется работа модуля анализа процессов. На следующем этапе выполняется фоновое отслеживание процесса контейнера и ожидание аварийного или запланированного завершения работы для последующего шифрования раздела контейнера.

Заключение

В результате разработки программного обеспечения для повышения безопасности криптозащищенного контейнера при помощи использования алгоритмов криптографии и модуля предиктивной работы контейнера был выявлен новый алгоритм, на основе которого представляется

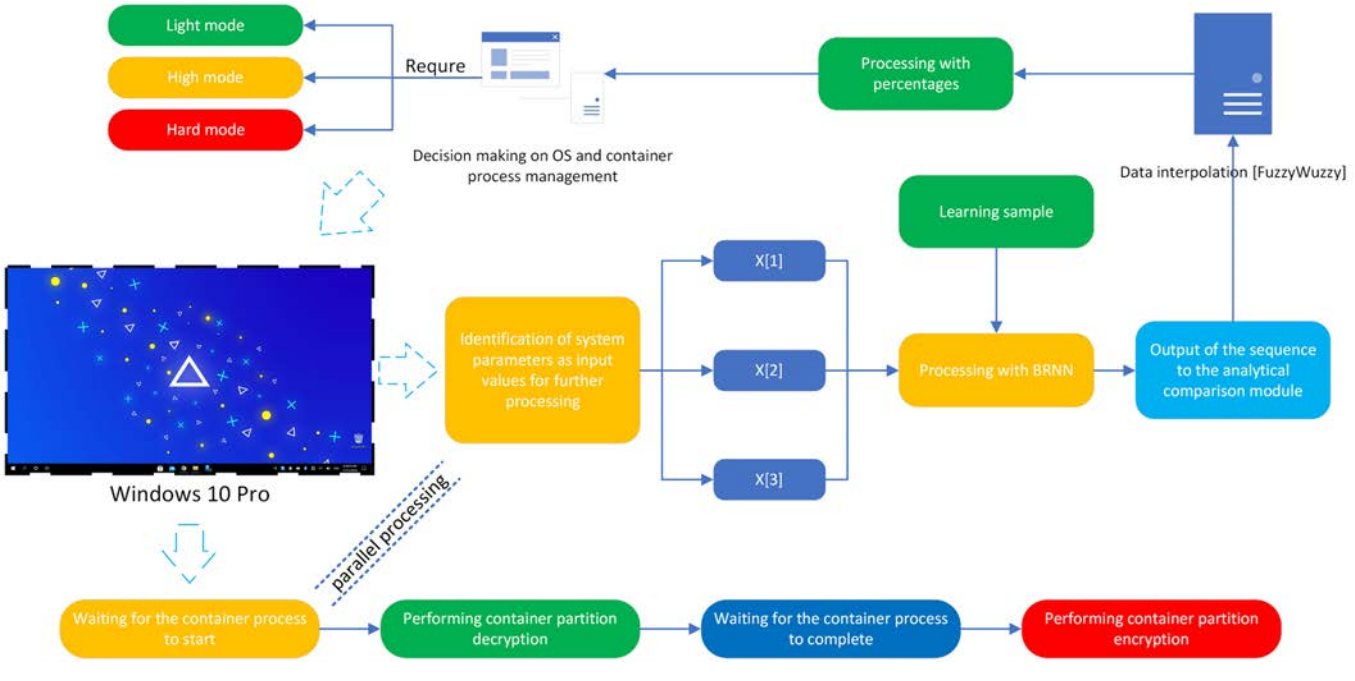


Рис. 4. Алгоритм взаимодействия нейронного модуля в разработанном ПО

возможным автоматизировать выполнение задач прикладного типа для организаций в сфере обеспечения безопасности. Интеграция двунаправленного алгоритма нейронной сети, изменённого для взаимодействия с выходными параметрами операционной системы, позволила определять в процессе работы факт превышения количества используемых ресурсов для дальнейшего принятия решений по устранению выявленной ошибки. Интерполяция выходных значений на основе нечетких правил, обрабатываемых при помощи модуля FuzzyWuzzy, позволила определить процентное соотношение возможности нарушения корректной работоспособности операционной системы и запущенного экземпляра процесса на основе выбора режима работы разработанного ПО. Также можно сказать, что фреймворк глубокого обучения PyTorch позволяет оптимизировать работу с нейронной моделью и обеспечить работу с вариативными аппаратными компонентами ОС.

Литература

1. *Dunkerley M., Tumbarello M.* Mastering Windows Security and Hardening: Secure and protect your Windows environment from intruders, malware attacks, and other cyber threats. 1st ed. Birmingham: Packt Publ., 2020. 572 p.

2. *Jordan K.* Mastering Windows Server 2019: The complete guide for IT professionals to install and manage Windows Server 2019 and deploy new capabilities. 2nd ed. Birmingham: Packt Publishing, 2019. 524 p.

3. *Mr. Tony V.R.* Building Virtual Machine Labs: A Hands-On Guide. 1st ed. South Carolina: CreateSpace Independent Publishing Platform, 2017. 600 p.

4. *Mike B., Harsey C., Martin G., Andrea M., Karel N., Paolo V.* The Complete VMware vSphere Guide: Design a virtualized data center with VMware vSphere 6.7. Birmingham: Packt Publishing, 2019. 768 p.

5. *Климов В.А.* Средства обеспечения ИБ в ОС семейства Windows Server // Наука, техника и образование. 2019. № 11 (64). С. 25–27.

6. *Syrewicze A., Siddaway R.* Pro Microsoft Hyper-V 2019: Practical Guidance and Hands-On Labs. 1st ed. New York: Apress, 2018. 410 p.

7. *Chris D.* Mastering Windows PowerShell Scripting: Automate and manage your environment using PowerShell Core 6.0. 3rd ed. Birmingham: Packt Publ., 2019. 626 p.

8. *Srivastava S.* Mastering Microsoft Windows Server Hyper V: Design Build and Manage a Virtualized Data Center. Chicago: Independently published, 2021. 264 p.

9. *Wes M.* Python for Data Analysis: Data Wrangling with Pandas, NumPy, and IPython. 2nd ed. Newton: O'Reilly Media, 2017. 550 p.

10. *Paul D., Harvey D.* Intro to Python for Computer Science and Data Science: Learning to Program with AI, Big Data and The Cloud. 1st ed. New York: Pearson, 2019. 880 p.

11. *Jack C., Ray C., Jack H. Sagar R.* Python API Development Fundamentals: Develop a full-stack web application with Python and Flask. 1st ed. Birmingham: Packt Publishing, 2019. 372 p.

12. *Banzal S.* XML Basics. New York: Mercury Learning & Information, 2020. 645 p.

13. *Jeff S., Manuel S., Richard D.* Windows 10 for Enterprise Administrators: Modern Administrators' guide based on Redstone 3 version. Birmingham: Packt Publishing, 2017. 314 p.

14. *Joshua H.* The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption. Princeton: Princeton University Press, 2018. 392 p.

15. *Кореневa А.М.* Оценка характеристик перемешивания хэш-функций семейства MD // ПДМ. Приложение. 2019. № 12. С. 107–110.

16. *Nielson S.J., Monson C.K.* Practical Cryptography in Python: Learning Correct Cryptography by Example. 1st ed. New York: Apress, 2017. 386 p.

17. *Stallings W.* Cryptography And Network Security, 7Th Edition. 7th ed. London: Pearson Education, 2017. 767 p.

18. *Himansu D., Chittaranjan P., Nilanjan D.* Deep Learning for Data Analytics: Foundations, Biomedical Applications, and Challenges. 1st ed. Cambridge: Academic Press, 2020. 218 p.

19. *Simeon K.* Recurrent Neural Networks with Python Quick Start Guide: Sequential learning and language modeling with TensorFlow. Birmingham: Packt Publishing, 2018. 122 p.

20. *Линдигрин А.Н.* Искусственные нейронные сети как основа глубинного обучения // Известия ТулГУ. Технические науки. 2019. № 12. С. 468–472.

21. *Singh H., Ahmad Y.L.* Deep Neuro-Fuzzy Systems with Python: With Case Studies and Applications from the Industry. 1st ed. New York: Apress, 2019. 275 p.

CRYPTOGRAPHIC DATA CONTAINERIZATION IN PROCESSING DEEP LEARNING NEURAL NETWORKS

ALEXANDER A. TYUTYUNNIK

Smolensk, Russia, tyutyunnik.aa@yandex.ru

ALEXEY I. LAZAREV

Smolensk, Russia, anonymous.prodject@gmail.com

KEYWORDS: hard disk drives; confidential information deletion; residual magnetization areas; intruder; magnetic force microscopy; channel for unauthorized information recovery; model of binary symmetric channel without memory.

ABSTRACT

Introduction: the existing development of methods for ensuring information security in the field of information technology allows you to control the confidentiality of personal data at variable levels. Hardware solutions can be portable cryptographic keys, as well as narrowly targeted biometric identification devices. Software solutions are methods of static verification using sequences and side-tools for deploying data virtualization systems. The main problem that stands out among the methods described above is the need for additional hardware that acts as tokens, infrared cameras, and biometric identification sensors. An alternative problem is the lack of security of

software solutions, since the presence of zero-day vulnerabilities can reduce security, which leads to the possibility of interception of confidential data by third parties. **Purpose of the research** is expressed in the analysis and development of software methods and algorithms for ensuring data security based on containerization methods. The developed software solution allows you to perform application tasks in a secure container, while the implemented authentication methods support the ability to identify an individual both using sequences and using the Windows Hello application programming interface. **Methods used:** security methods and algorithms aimed at implementing a unique cryptographic algorithm. **The results** of the studied methods and algorithms for scanning a bounded shell allow us to variatively select the optimal outcomes of internal process instances along with the implementation of cryptographic methods. Application software is based on the joint use of virtualization tools and methods of interaction through neural network technologies. The isolation of this solution from alternative methods lies in the possibility of using the container without significant hardware resources and lack of primary knowledge in configuring the software module. **Practical significance** lies in the possibility of using methods and algorithms in the construction of secure jobs in small and medium-sized businesses.

REFERENCES

1. Dunkerley M., Tumbarello M. *Mastering Windows Security and Hardening: Secure and protect your Windows environment from intruders, malware attacks, and other cyber threats.* 1st ed. Birmingham: Packt Publishing, 2020. 572 p.
2. Jordan K. *Mastering Windows Server 2019: The complete guide for IT professionals to install and manage Windows Server 2019 and deploy new capabilities.* 2nd ed. Birmingham: Packt Publishing, 2019. 524 p.
3. Mr. Tony V.R. *Building Virtual Machine Labs: A Hands-On Guide*. 1st ed. South Carolina: CreateSpace Independent Publishing Platform, 2017. 600 p.
4. Mike B., Harsey C., Martin G., Andrea M., Karel N., Paolo V.*The Complete VMware vSphere Guide: Design a virtualized data center with VMware vSphere 6.7.* Birmingham: Packt Publishing, 2019. 768 p.
5. Klimov V.A. Information security tools in the windows server family. Nauka, tehnika i obrazovanie [Science, technology and education]. 2019. No. 11 (64). Pp. 25–27. (In Rus)
6. Syrewicze A., Siddaway R. *Pro Microsoft Hyper-V 2019: Practical Guidance and Hands-On Labs.* 1st ed. New York: Apress, 2018. 410 p.
7. Chris D. *Mastering Windows PowerShell Scripting: Automate and manage your environment using PowerShell Core 6.0.* 3rd ed. Birmingham: Packt Publishing, 2019. 626 p.
8. Srivastava S. *Mastering Microsoft Windows Server Hyper V: Design Build and Manage a Virtualized Data Center.* Chicago: Independently published, 2021. 264 p.
9. Wes M. *Python for Data Analysis: Data Wrangling with Pandas, NumPy, and IPython*. 2nd ed. Newton: O'Reilly Media, 2017. 550 p.
10. Paul D., Harvey D. *Intro to Python for Computer Science and Data Science: Learning to Program with AI, Big Data and The Cloud*. 1st ed. New York: Pearson, 2019. 880 p.
11. Jack C., Ray C., Jack H. Sagar R. *Python API Development Fundamentals: Develop a full-stack web application with Python and Flask*. 1st ed. Birmingham: Packt Publishing, 2019. 372 p.
12. Banzal S. *XML Basics*. New York: Mercury Learning & Information, 2020. 645 p.
13. Jeff S., Manuel S., Richard D. *Windows 10 for Enterprise Administrators: Modern Administrators' guide based on Redstone* 3 version. Birmingham: Packt Publishing, 2017. 314 p.
14. Joshua H. *The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption*. Princeton: Princeton University Press, 2018. 392 p.
15. Koreneva A.M. Estimation of the mixing characteristics of hash functions of the MD family. PDM. Prilozhenie 2019 [PDM. Application 2019]. No. 12. Pp. 107–110. (In Rus)
16. Nielson S.J., Monson C.K. *Practical Cryptography in Python: Learning Correct Cryptography by Example*. 1st ed. New York: Apress, 2017. 386 p.
17. Stallings W. *Cryptography And Network Security, 7Th Edition*. 7th ed. London: Pearson Education, 2017. 767 p.
18. Himansu D., Chittaranjan P., Nilanjan D. *Deep Learning for Data Analytics: Foundations, Biomedical Applications, and Challenges*. 1st ed. Cambridge: Academic Press, 2020. 218 p.
19. Simeon K. *Recurrent Neural Networks with Python Quick Start Guide: Sequential learning and language modeling with TensorFlow.* Birmingham: Packt Publishing, 2018. 122 p.
20. Lindigrin A.N**.** Artificial neural networks as a foundation for deep learning. Izvestija TulGU. Tehnicheskie nauki [Izvestiya TulGU. Technical science]. 2019. No. 12. Pp. 468–472. (In Rus)
21. Singh H., Ahmad Y.L. *Deep Neuro-Fuzzy Systems with Python: With Case Studies and Applications from the Industry.* 1st ed. New York: Apress, 2019. 275 p.

INFORMATION ABOUT AUTHORS:

Tyutyunnik A.A., PhD, Associate Professor at the Department of Information Technology in Economics and Management, Branch of the National Research University Moscow Power Engineering Institute in Smolensk;

Lazarev A.I., Student, Branch of the National Research University Moscow Power Engineering Institute in Smolensk.

For citation: Tyutyunnik A.A., Lazarev A.I. Cryptographic data containerization in processing deep learning neural networks. *H&ES Research*. 2021. Vol. 13. No. 3. Pp. 68–75. Doi: 10.36724/2409-5419-2021-13-3-68-75 (In Rus)

ТРЕБОВАНИЯ К ПРЕДСТАВЛЕНИЮ МАТЕРИАЛОВ

Редакция журнала H&ES Research принимает к публикации статьи на русском и английском языках. Предоставляемая рукопись должна быть актуальной, обладать новизной, отражать постановку задачи, содержать описание основных результатов исследования, выводы, а также соответствовать указанным ниже правилам оформления. Текст должен быть тщательно вычитан автором, который несет ответственность за научнотеоретический уровень публикуемого материала.

Статья предоставляется в электронном виде, единым файлом, имеющим следующую структуру: заглавие статьи, сведения об авторах, аннотация, ключевые слова, текст статьи (включая иллюстрации, таблицы и формулы), пристатейный список литературы, англоязычный блок. Также представляется отдельная папка с экспортированными изображениями рисунков в формате TIFF, EPS по требованиям указанным в п.7.

К статье прилагается экспертное заключение о возможности опубликования статьи в открытой печати и две рецензии кандидатов или докторов наук по профилю планируемой публикации материалов (сканированные копии в электронном виде).

Все материалы высылаются электронной почтой в адрес журнала: HT-ESResearch@yandex.ru.

1. **Статья подготавливается** в редакторе MS Word. Шаблон статьи можно скачать на сайте журнала www.h-es.ru.

2. **Данные об авторе:** фамилия, имя, отчество, ученая степень, звание, должность и полное название организации – места работы, город, страна, адрес электронной почты и почтовый адрес каждого автора полностью.

3. **Объем аннотации** 200–250 слов. Аннотация должна быть информативной (не содержать общих слов), без сокращений, структурированной, отражать основное содержание статьи: предмет, цель, методологию проведения исследований, результаты исследований, область их применения, выводы. Приводятся основные теоретические и экспериментальные результаты, фактические данные, обнаруженные взаимосвязи и закономерности. Выводы могут сопровождаться рекомендациями, оценками, предложениями, гипотезами, описанными в статье. Предложения должны начинаться словами: показано, получено, исследовано, предсказано и т.д. и т.п.

4. **Ключевые слова:** от 5 до 7 слов (словосочетаний), разделенных точкой с запятой.

5. **Объём статьи** без аннотации – от 15 до 30 тыс. знаков с пробелами. Рисунки и таблицы в объеме статьи не учитываются.

6. **Формульные выражения** выполняются в редакторе Math Type. Формулы нумеруются в круглых скобках, источники – в прямых. Нумерация формул и приведение в списке источников, на которые нет ссылок по тексту, не допускается. Длина формулы в одну строчку 8–9 см.

Простые формулы и буквенные обозначения величин следует писать в строку обычным текстом. В формулах использовать только буквы латинского и греческого алфавита!

Размеры шрифтов (Size) предварительно перед набором первой формулы установить (в MathType) следующие: кегль основной – 10, крупный индекс – 7, мелкий индекс – 5, крупный символ – 12, мелкий символ – 8. Формулы, не содержащие специальных математических символов, должны быть набраны в тексте (в формате Word). Греческие обозначения, скобки (квадратные и круглые) и цифры всегда набираются прямым шрифтом. Латинские буквы набираются курсивом как в формулах, так и в тексте, кроме устойчивых форм (max, min, cos, sin, tg, log, exp, det …).

Нельзя использовать сканированные формулы! Все формулы должны быть набраны вручную!

7. **Рисунки и таблицы** в статье должны быть пронумерованы и снабжены подписями, в тексте статьи должны иметься ссылки на каждый рисунок и таблицу (рис.1 и табл.1). Если рисунок или таблица единственные в статье, то их не нумеруют.

Рисунки должны быть четкими, с хорошо проработанными деталями. Избегать текстовых надписей на иллюстрациях. Заменять их цифровыми обозначениями, которые поясняются в подписи или в основном тексте. Все рисунки прилагаются в виде отдельных файлов в формате TIFF, EPS с разрешением не менее 300 dpi для оригинального размера в печатном издании (для больших рисунков ширина от 14 до 20 см, для маленьких от 7 до 9 см).

8. **Список литературы:** от 15 до 50 наименований. Из них самоцитирований не должно быть более 25%. В числе источников желательно не менее 50 % иностранных источников (для статей на английском языке – 15% российских). Состав источников должен быть актуальным и содержать не менее 8 статей из научных журналов не старше 10 лет, из них 4 – не старше 3 лет.

Ссылки должны быть только на статьи, патенты, книги и статьи из сборников трудов. В списках литературы не размещать ГОСТЫ, рекомендации, диссертации, авторефераты и другую нормативную и непериодическую документацию. Эти данные можно указывать в теле статьи в скобках или в виде постраничных сносок (если автор непременно хочет указать нормативный документ или сослаться на свою диссертацию). Список литературы оформляется в соответствии с ГОСТ 7.052008. **Образец оформления списка литературы размещен на сайте журнала www.h-es.ru.**

9. **На английском языке** предоставляется: название статьи, фамилия, имя, отчество, информация об авторах (должность, ученая степень, ученое звание, место работы), город, страна и электронный адрес всех авторов полностью, аннотация, ключевые слова и списки литературы.

Все названия издательств и журналов должны быть транслитерированы, а не переведены. Названия организаций в списках литературы (Труды Академии...) должны быть четко выверены с данными организации и иметь официальное английское наименование, которое указано на их сайте или также транслитерированы. Образец оформления списка литературы размещен на сайте журнала www.h-es.ru.

10. **Структура статьи на английском языке**

Introduction (введение)

Materials and methods (материалы и методы).

Results and Discussions (результаты и обсуждение).

Conclusions (вывод)

Acknowledgements (благодарности, необязательный раздел)

References (ссылки на использованную литературу)

На руском языке предоставляется: название статьи, фамилия, имя, отчество, информация об авторах (должность, ученая степень, ученое звание, место работы), город, страна и электронный адрес всех авторов полностью, аннотация, ключевые слова и списки литературы.

Внимание! Редакция оставляет за собой право отклонить представленные материалы, оформленные не по указанным правилам.