ВЕСТНИК

МОРСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА

Серия

Автоматическое управление, математическое моделирование и информационные технологии

Вып. 78/2017

Вестник Морского государственного университета имени адмирала Г. И. Невельского. Серия: Автоматическое управление, математическое моделирование и информационные технологии. Вып. 78/2017 – Владивосток: Мор. гос. ун-т, 2017 – 147 с.

ISBN 978-5-8343-1062-4

Учредитель журнала – Морской институт
информационных технологий
МГУ имени адмирала Г.И. Невельского

ISBN 978-5-8343-1062-4

УДК 004.056.5

Белоножко Роман Алексеевич,
магистр 1-го года обучения, кафедра информационных систем управления, ДВФУ, г. Владивосток
Мазур Максим Владимирович,
магистр 1-го года обучения, кафедра информационных систем управления, ДВФУ, г. Владивосток

ОБЗОР ПРОБЛЕМ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМЕ «1С:ПРЕДПРИЯТИЕ»

«1С:Предприятие» представляет собой современную, универсальную систему автоматизации экономической и организационной деятельности предприятия, которая позволяет контролировать все стадии товарооборота – от закупки и поступления товара до его реализации. При этом, система «1С:Предприятие» является открытой, и не только позволяет использовать типовые механизмы, предусмотренными разработчиками фирмы 1С, но также разрабатывать свои или дорабатывать существующие. Это облегчает проводить адаптацию системы под нужды конкретного предприятия.

Защита информации представляет собой комплексную задачу и зависит не только от технических и программных средств, но и от административных действий и правил компании. Важно уточнить, что система «1С:Предприятие» поддерживает два режима работы: файловый и клиент-серверный. Файловый вариант предназначен для работы небольшого числа пользователей, обладает малыми возможностями по масштабируемости и защите данных. Клиент-серверный вариант предназначен для работы в масштабах предприятия и реализован на основе трехуровневой архитектуры «клиент-сервер». На рисунке 1 представлена схема клиент-серверного варианта работы.

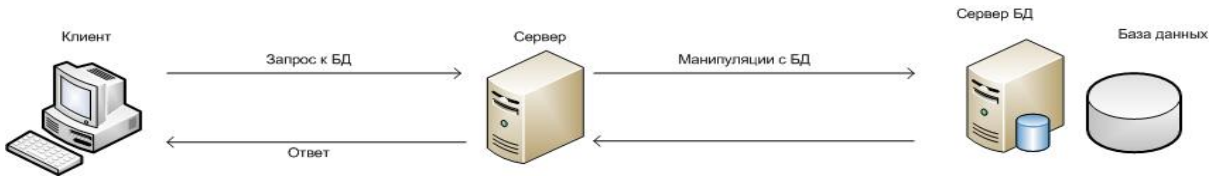

Рис. 1. Схема клиент-серверной архитектуры «1С:Предприятие»

В данной архитектуре обычно определяет три взаимодействующих между собой части системы. Клиентское приложение используется для организации пользовательского интерфейса, и также может исполнять код на встроенном языке 1С. Сервер предназначен для выполнения алгоритмов разработчика, передачи запросов от клиента к базе данных и возвращения результатов. Третья часть системы – сервер баз данных (БД). Он поставляется сторонними производителями и предназначен для ведения и органи-

зации баз данных. В настоящее время, система может работать со следующими серверами баз данных: MS SQL Server, Oracle Database др.

Таким образом, в клиент-серверной архитектуре можно выделить три основных участках, на которых обеспечивается защита информации:

1. клиент – сервер 1С;
2. сервер 1С – сервер БД;
3. пользователь системы.

Рассмотрим основные угрозы безопасности, которые существуют при работе.

Доступ пользователей к административным действиям конфигуратора. В конфигураторе администраторы и программисты дорабатывают программный и настраивают конфигурацию. У каждого пользователя в системе должна быть своя учетная запись. Она может принадлежать к нескольким ролям. Роль – это набор полномочий, которые предоставляют права на чтение, редактирование объектов в системе. Существуют роли, которые предоставляют пользователям права на такие действия, как выгрузку текущей конфигурации со всеми данными в отдельный файл, который потом можно записать на съемный носитель. В дальнейшем, злоумышленник может распоряжаться этой информацией как хочет. Важно понимать, насколько целесообразно наличие у пользователя таких ролей. Необходимо определиться, какими правами должен обладать администратор и лишить этих прав остальных пользователей. Иначе, такой пользователь является потенциальной угрозой безопасности. Как показывает практика, вероятность возникновения такой угрозы довольно высока и возникает на участке «пользователь системы».

Отсутствие разграничений доступа в режиме «1С:Предприятие». В одной системе могут работать пользователи различных направлений деятельности. Поэтому важно, чтобы например работники, допустим склада, не имели доступа к данным о заработной плате сотрудников компании.

Несанкционированный доступ к данным сервера СУБД. Если не минимизировать данную угрозу, то впоследствии злоумышленник может получить полный доступ к БД, хранящимся на сервере.

Несанкционированный доступ к файлам кластера серверов. Злоумышленник может получить пароли и общую информацию для подключения к серверу СУБД. Это может привести к тому, что ему станут полностью доступны БД системы.

Уязвимости операционной системы, СУБД. Злоумышленник, используя данные уязвимости, при наличии удаленного доступа к серверам из Интернета, может получить доступ к данным. Необходимо следить за сообщениями разработчиков об обнаружении уязвимостей и регулярно обновлять ПО.

Слабые пароли. Даже самые современные методы защиты могут оказаться бессильными, если пароль к учетной записи не держать в секретности, потому что они становятся основной целью злоумышленника.

Перехват информации. Возможным последствием является полный перехват всего сетевого трафика, расшифровав который, можно получить информацию о работе системы.

Таким образом, задача обеспечения информационной безопасности баз данных системы «1С:Предприятие» является актуальной и требует разработки практических рекомендаций по реализации механизмов обеспечения безопасности и их практической реализации.

Список литературы

1. Ирина Баймакова, Александр Новиков, Алексей Рогачев, Агиль Хыдыров. Обеспечение защиты персональных данных (+ CD-ROM). // 1С-Паблишинг. 2011. 272с.

2. Механизмы обеспечения безопасности в 1С:Предприятии 8.1. [Электронный ресурс] // Режим доступа: https://its.1c.ru/db/metod8dev#content:5816:hdoc. – Загл. с экрана. – Яз. рус.

УДК 621.311.016.2

Борисов Сергей Иванович,

к.т.н, доцент, декан ФЭИТ, МГУ им. адм. Г.И. Невельского

УПРАВЛЯЕМЫЙ РЕАКТОР ДЛЯ АВТОМАТИЧЕСКОГО ФИЛЬТРОКОМПЕНСАТОРА

В качестве фильтрокомпенсатора (далее – ФК) в современных автономных электроэнергетических установках (далее – ЭЭУ) широко применяется реактированная конденсаторная батарея, которая генерирует в сеть реактивную энергию по первой гармонике, подавляя при этом высшие гармоники тока, таким образом снижает коэффициент несинусоидальности и позволяет исключить резонансное повышение гармоник тока [1] .

Управляемый реактор является одним из основных элементов автоматической следящей системы настройки ФК в резонанс по $к$ гармонике тока путем плавного изменения индуктивности L_p за счет подмагничивания постоянным током в обмотке управления ОУ. На рис. 1, *а* изображена реактированная конденсаторная батарея C_p в однофазном исполнении.

Управляемые реакторы могут выполняться с продольным, кольцевым и поперечным подмагничиванием. В предлагаемом ФК [1] целесообразно применять реактор с поперечным подмагничиванием, который имеет пониженные потоки рассеяния, допускает пофазное регулирование, позволяет получить линейные вольт-амперные характеристики и повышенное быстродействие.

Мощность реактора составляет около 5% от мощности конденсаторной батареи. При фазной мощности конденсаторной батареи Q=17,5 квар, фазном напряжении $U_ф$=220 В частоте сети f=50 Гц ток реактора составляет I_p=79,5 А. Для фильтрации пятой гармоники тока $к$=5 индуктивность реак-

тора должна быть $L_{рн}$ = 0,00036 Гн. Требуемый диапазон регулирования индуктивности реактора составляет ±20%, глубина регулирования $к_р$ =1,4, магнитная индукция в стержне без подмагничивания принимается B_m =1,05 Тл. При этом масса реактора составила 6,9 *кг*. Индуктивность реактора при пренебрежении активным сопротивлением реактора можно определить

$$L_p = U_p / I_p,$$

где U_p =0,05 $U_ф$ – напряжение на реакторе.

Зависимость индуктивности реактора L_p от тока подмагничивания I_y показана на рис.1,б.

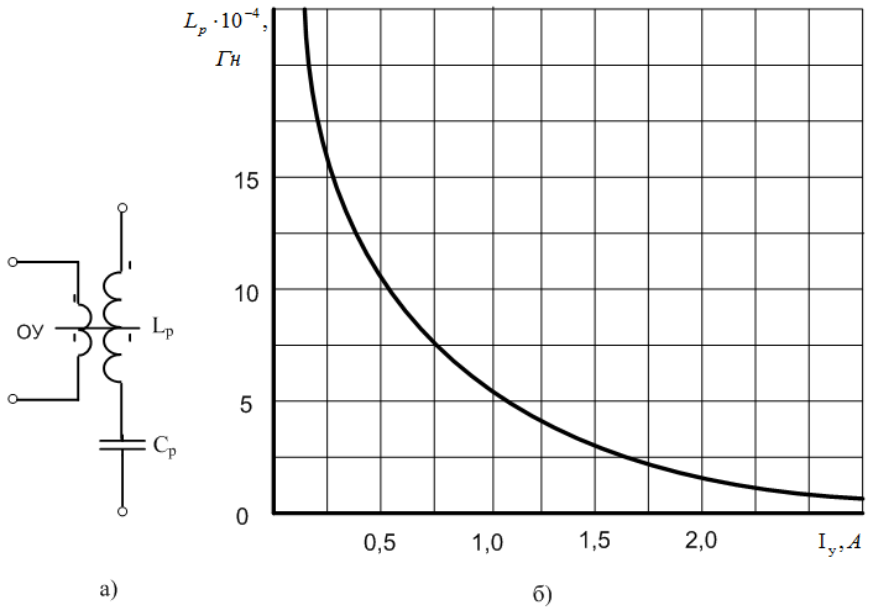

Рис. 1.

Номинальный ток подмагничивания, при котором индуктивность реактора составляет L_p = 0,00036 Гн равен $I_{ун}$=1,35 А .При изменении тока подмагничивания от I_{min}=1,18 А до I_{max}=1,51 А индуктивность реактора изменяется соответственно от L_{pmax}=0,00043 Гн до L_{pmin}=0,00029 Гн, что составляет ±20% от $L_{рн}$, что удовлетворяет требуемому диапазону регулирования индуктивности реактора.

Список литературы

1. Борисов С.И. Автоматический фильтрокомпенсатор для подавления высших гармоник.-Материалы пятой Всероссийской научно-практической конференции.- Пермь, Изд-во Перм. нац. исслед. политехн. ун-та, 2016

2. Дорожко Л.И., Либкинд М.С. Реакторы с поперечным подмагничиванием.- М., Энергия, 1977

УДК 004.056.5

Гончаров Сергей Михайлович,
к. ф.-м. н., доцент, МГУ им. адм. Г.И. Невельского,
e-mail: sgprim@smtp.ru
Боршевников Алексей Евгеньевич,
ассистент кафедры ИБ, ДВФУ,
e-mail: LAdG91@mail.ru

ПРОЦЕДУРА ОЦЕНКИ КАЧЕСТВА НЕЙРОСЕТЕВОГО ПРЕОБРАЗОВАТЕЛЯ "БИОМЕТРИЯ - КОД ДОСТУПА" НА ОСНОВЕ ЭЭГ

Обеспечение информационной безопасности является важной задачей для любого государства. Большое значение в настоящее время приобретают угрозы, исходящие от различных террористических и экстремистских организаций [1]. В связи с этим возрастает потребность в обеспечении безопасности различных объектов и, особенно, критически важных объектов. Такие объекты требуют технологий, обеспечивающих высокий уровень безопасности, в частности, систем высоконадежной биометрической аутентификации.

Под системами высоконадежной биометрической аутентификацией понимаются системы биометрической аутентификации с приемлемой вероятностью ошибок первого рода и гарантированно малой вероятностью ошибок второго рода, сопоставимой по своему значению с вероятностью случайного подбора кода неизвестного криптографического ключа при малом числе попыток подбора [2]. Подобные системы сильно зависят от конфиденциальности биометрических данных, обрабатываемых ими. Электроэнцефалограмма (ЭЭГ) выделяется среди других характеристик своей высокой степенью конфиденциальности. В настоящее время ведутся активные исследовательские работы по созданию системы высоконадежной биометрической аутентификации на основе данных ЭЭГ [3,4].

В качестве решения для реализации подобной системы была выбрана схема нейросетевого преобразователя "Биометрия – код доступа". Подобный выбор обусловлен результатами исследований по применению этой схемы в создании систем высоконадежной биометрической аутентификации на основе других биометрических характеристик [5]. Также немаловажным фактором в выборе данной схемы является наличие стандартов систем высоконадежной биометрической аутентификации, которые основываются на нейросетевых преобразователях "Биометрия - код доступа" [2,6].

Одной из важных задач, которая возникает при анализе качества, разрабатываемой системы высоконадежной биометрической аутентифика-

ции, является сравнение некоторых характеристик с требованиями, устанавливаемыми стандартами.

Согласно стандарта ГОСТ Р 52633.0–2006 для преобразователей "Биометрия - код доступа" устанавливаются определенные характеристики и к ним предъявляются следующие требования [2].

1. Стабильность выходного кода. Необходима близость к равновероятным состояниям "0" и "1" во всех разрядах выходного кода при подаче на вход преобразователя случайных биометрических образов «Чужой». Допускаются отклонения вероятностей в пределах $(0,5 \pm 0,1)$.

2. Среднее значение модулей коэффициентов парной корреляции. Значения коэффициентов парной корреляции в качестве наиболее вероятного должны иметь нулевое значение. Допустимое среднее значение модулей коэффициентов парной корреляции – не более 0,15 при статистической выборке в 300 примеров образов «Чужой». Коэффициент парной корреляции имеет вид [7]:

$$r_{XY} = \frac{S_{XY}}{S_X S_Y} = \frac{\sum_i (x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_i (x_i - \overline{x})^2 \sum_i (y_i - \overline{y})^2}}, \quad (1)$$

где S_{XY} - выборочная ковариация случайных величин X и Y; S_X и S_Y - выборочные стандартные отклонения случайных величин X и Y; x_i - i-й элемент выборки случайной величины X; y_i - i-й элемент выборки случайной величины Y; $\overline{x}$ – среднее значение выборки случайной величины X; $\overline{y}$ – среднее значение выборки случайной величины Y.

Под случайной величиной для нейросетевых преобразователей понимается значение выходного кода преобразователя.

3. Математическое ожидание расстояния Хэмминга. Математическое ожидание расстояния Хемминга между ключами, полученными от образов «Чужой», и ключами для образа «Свой» должно быть близко к половине длины ключа.

Для оценки качества нейросетевого преобразователя, т. е. получения его характеристик и сравнения их с требованиями стандартов проводится следующая процедура.

1. Оценивание неполноты базы естественных биометрических образов "Чужой". Неполнота базы приводит к снижению достоверности тестирования, но в большинстве случаев использование таких баз допустимо. При формировании неполной базы из N биометрических образцов «Чужой» показатель неполноты базы определяют по формуле:

$$\phi = \frac{\log(N)}{\log(N_{Полн})}, \quad (2)$$

где $N_{Полн}$ – количество образцов в полной базе "Чужой". Приблизительно данное значение берется равное 10^{12}.

При дальнейшем тестировании неполную базу можно многократно увеличивать за счет дополнения ее синтетическими биометрическими образами. Количество дополнительных синтетических образов рассчитывают по формуле:

$$N_{синт} \approx N^{\frac{1}{\phi}} - N. \quad (3)$$

2. Дополнение базы образов "Чужой" синтетическими образами. В силу сложности сбора биометрических данных стандарты предусматривают дополнение базы естественных образов синтетическими [6].

3. Моделирование работы нейросетевого преобразователя "Биометрия - код доступа" и получение необходимых для расчета характеристик данных.

4. Сравнение характеристик преобразователя "Биометрия - код доступа" с требованиями некоторого эталона (стандарта).

Применим предложенную процедуру к оценке качества нейросетевого преобразователя "Биометрия - код доступа" на основе ЭЭГ.

В качестве биометрических данных была взята база данных ЭЭГ P300, сформированная при мысленной концентрации пользователей на меняющихся символах [3]. Использованная структура нейросетевого преобразователя соответствует структуре преобразователя, применявшегося для биометрической аутентификации на основе потенциала движения мышц глаз [4]. Было рассчитано, что необходимое количество синтетических образцов в базе "Чужой" составляет $N_{синт} \approx 10^{10}$. В силу того, что такое количество синтетических образцов является достаточно большим числом, было принято решение об использовании минимального значения размера базы образов "Чужой" необходимого для тестирования преобразователя – 300 образцов [6]. Были получены следующие результаты (Таблица 1).

Таблица 1

Сравнение характеристик преобразователя "Биометрия - код доступа с требованиями стандарта ГОСТ Р 52633.0–2006

Наименование характеристики	Характеристики преобразователя	Требования стандарта ГОСТ Р 52633.0
Математическое ожидание расстояния Хэмминга	123	(128 ± 6)
Среднее значение модулей коэффициентов парной корреляции	$0,06$	$\leq 0,15$
Стабильность выходного кода	$X = [0,403; 0,597]$	$X = [0,4; 0,6]$

Анализируя данные, приведенные в таблице, можно говорить, что нейросетевой преобразователь "Биометрия - код доступа" удовлетворяет требованиям стандарта ГОСТ Р 52633.0. Стоит отметить несколько важных аспектов полученных результатов.

1. Значение математического ожидания расстояния Хэмминга свидетельствует о том, что в среднем получаемые значения выходного ключа для образа "Чужой" соответствуют случайному ключу.

2. Среднее значение модулей коэффициентов парной корреляции показывает, что выходы преобразователя слабо связаны между собой. Данный факт затрудняет злоумышленнику возможность анализа выходных значения и построения предположений о величинах данных значений.

3. Оценка стабильности выходного кода показывает, что значения координат выходного кода для образа "Чужой" появляются в целом равновероятно, то есть выход для образа "Чужой" является случайным.

Несмотря на то, что характеристики нейросетевого преобразователя "Биометрия - код доступа" на основе ЭЭГ соответствуют требованиям стандарта, стоит отметить, что данные значения были получены на малом объеме базы "Чужой". Дальнейшие исследования предполагают генерацию базы "Чужой" необходимого объема и проведение процедуры оценки качества нейросетевого преобразователя.

Список литературы

1. Доктрина информационной безопасности Российской Федерации [утв. Указом Президента Российской Федерации от 5 декабря 2016 г. N 646]. – М.: Кремль, 2016. – 8 с.

2. Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации: ГОСТ Р52633.0–2006. – Введен впервые; введ. 27.12.2006. – М.: Стандартинформ, 2007. – 25 с.

3. Гончаров С.М., Боршевников А.Е. Построение нейросетевого преобразователя "Биометрия - код доступа" на основе параметров визуального вызванного потенциала электроэнцефалограммы / С.М. Гончаров, А.Е. Боршевников // Доклады Томского государственного университета систем управления и радиоэлектроники: Научный журнал. – Томск: Изд–во ТУСУР, 2014. – № 2. – С. 51–55.

4. Гончаров С.М. Восстановление секретного ключа на основе электроэнцефалограммы при движении глаз с закрытыми веками. / Гончаров С.М., Боршевников А.Е., Михайлов А.Г., Апальков А.Ю. // Журнал «Информация и безопасность». Том. 19, часть 1. Воронеж: ВГТУ, 2016. – С. 114-117.

5. Иванов, А. И. Нейросетевые алгоритмы биометрической идентификации личности. Кн. 15: Монография / А. И. Иванов. – М.: Радиотехника, 2004. – 144 с.

6. Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации: ГОСТ Р 52633.2–2010. – Введен впервые; введ. 30.09.2010. – М.: Стандартинформ, 2011. – 17 с.

7. Статистические методы. Вероятность и основы статистики. Термины и определения: ГОСТ Р 50779.10–2000. – Введен впервые; введ. 29.12.2000. – М.: Стандартинформ, 2008. – 46 с.

УДК 004.056.5

Гончаров Сергей Михайлович,
к. ф.-м. н., доцент, МГУ им. адм. Г.И. Невельского,
e-mail: sgprim@smtp.ru
Боршевников Алексей Евгеньевич,
ассистент кафедры ИБ, ДВФУ,
e-mail: LAdG91@mail.ru

РАСШИРЕННАЯ МОДЕЛЬ НЕЙРОСЕТЕВОГО ПРЕОБРАЗОВАТЕЛЯ "БИОМЕТРИЯ - КОД ДОСТУПА" НА ОСНОВЕ ЭЭГ

Исследование систем биометрической аутентификации имеет большое значение в области информационной безопасности. Важной задачей, которая возникает при исследовании подобных систем, является получение численных характеристик систем. Особенно это важно при разработке систем высоконадежной биометрической аутентификации, где необходимо контролировать выходное значение ошибки второго рода.

При исследовании для получения характеристик подобных систем прибегают к математическому моделированию. При моделировании систем высоконадежной биометрической аутентификации важный вклад в модель вносят выбор характеристики на основе, которой проходит аутентификация, метода выделения биометрических параметров из характеристики, а также механизма, производящего классификацию пользователей. Для того, чтобы математическую модель можно было применять для исследований, необходимо, чтобы она удовлетворяла некоторому набору свойств. Выделяют следующие свойства математических моделей [1]: полнота, точность, адекватность, продуктивность, экономичность, робастность, наглядность.

Для принятия математической модели необходимо выполнение большей части перечисленных свойств.

Исследование систем высоконадежной биометрической аутентификации на основе электроэнцефалограммы (ЭЭГ), основанных на больших нейронных сетях (нейросетевых преобразователях «Биометрия – код доступа»), проводится в течение нескольких лет во Владивостоке. При проведении этих работ была разработана усеченная математическая модель преобразователя, в которой были приведены не все параметры и элементы [2,3]. Опишем расширенную модель нейросетевого преобразователя, включающую в себя дополнительные элементы.

Будем рассматривать модель двухслойного нейронной сети, для которой проводились исследования.

Входными значениями модели будут:

1. I – общее количество электродов электроэнцефалографа;
2. $S_{Свой}, S_{Чужой}$ – базы биометрических данных легитимного пользователя (Свой) и злоумышленника (Чужой);
3. $N_{Свой}, N_{Чужой}$ – количество образцов биометрических данных в базах "Свой" и "Чужой";
4. J – количество выбираемых для анализа значений биометрической характеристики;
5. L, R – количество нейронов в слоях первого и второго слоев нейросетевого преобразователя;
6. $\overline{K}_1$ – вспомогательный ключ, используемый для обучения первого слоя нейросетевого преобразователя. Имеет следующий вид:

$$\overline{K}_1 = \{k_{1,l}\}, k_{1,l} \in \{-1;1\}, 1 \le l \le L. \quad (1)$$

7. $\overline{K}_2$ – восстанавливаемый ключ. Имеет следующий вид:

$$\overline{K}_2 = \{k_{2,r}\}, k_{2,r} \in \{0;1\}, 1 \le r \le R. \quad (2)$$

8. $PRNG()$ – псевдослучайный генератор;
9. IV – инициализирующий вектор.

ЭЭГ представляет собой нечеткий сигнал, снимаемый по нескольким каналам и изменяющийся во времени, который сложно описывается математически. По этой причине мы будем считать, что сигнал ЭЭГ это набор функций с каналов электроэнцефалографа, зависящих от времени.

$$\overline{s} = \{s_i(t)\}, 1 \le i \le I, \quad (3)$$

где i – номер электрода, с которого снята ЭЭГ.

Совокупность этих функций составляют базы электроэнцефалограмм "Свой" и "Чужой".

Для обработки нейронной сетью нельзя использовать функции, поэтому из функций принято выделять, некоторые их характеристики. Данные характеристики считают значениями биометрических параметров. В качестве выделения мы ведем функцию:

$$F(\overline{s}) = \{F(s_i(t))\} = \{\overline{a}_i\}, 1 \le i \le I, \quad (4)$$

где $\overline{a}_i$ – биометрический вектор, используемый в нейронной сети.

Данная функция обычно является комплексной и состоит из нескольких. Приведем пример подобного использования функции выделения параметров.

Рассмотрим функцию выделения параметров, применявшуюся в исследованиях [3]. В качестве метода выбора параметров было предложено использовать разложение в ряд Фурье:

$$a_{ik} = \sum_{n=0}^{N} s_i(t_{res}) e^{\frac{2\pi i}{N} k \cdot res}, k = \overline{0, RES}, \quad (5)$$

где RES - выбранное количество отсчетов для дискретизации функции; t_{res} – значение времени, соответствующее отсчету.

После этого коэффициенты отбрасываются, не удовлетворяя $10° < \arg a_{ik} < 90°$. Накладывая это условие, мы имеем в виду, что мы анализируем только неубывающие всплески ЭЭГ. Из остальных значений выбраны значения максимальной амплитуды коэффициентов j и следующая векторная форма:

$$\overline{a}_i = \{a_{ij}\}, \tag{6}$$

$$a_{ij} = \max_{a_i} |a| \cdot \cos(\arg a) : 10° < \arg a_{ik} < 90°, 1 \le i \le I, 1 \le j \le J, k = \overline{0, RES} \tag{7}$$

Таким образом, к примеру, описывается функция выделения параметров ЭЭГ.

Для биометрических параметров вводится ряд характеристик: стабильность биометрического параметра $c(a_i)$, показатель уникальности биометрического параметра $u(a_i)$, показатель качества биометрического параметра $q(a_i)$.

В случае описания нейросетевого преобразователя необходимо описать нейронную сеть. В общем случае это можно сделать следующим образом:

$$NET(a_i, \overline{w}_l, \overline{W}_r, \overline{net}_l, \Delta_r) = \overline{K}_{rest}, 1 \le i \le I, 1 \le l \le L, 1 \le r \le R, \tag{8}$$

$$\overline{K}_{rest} = \{k_r\}, \tag{9}$$

где $\overline{net}_l$ – вектор связей нейрона l; $\overline{w}_i$ – вектор весовых коэффициентов первого слоя; $\overline{W}_r$ – вектор весовых коэффициентов второго слоя; Δ_r - коэффициент использования; $\overline{K}_{rest}$ – восстанавливаемый преобразователем ключ.

Опишем нейронную сеть более подробно. Для описания первого слоя введем следующее значение:

$$v_i = \overline{a}_i \cdot \overline{w}_i, 1 \le i \le I. \tag{10}$$

Это нормированная величина, которая подается на входы сумматоров с электрода i. Составим вектор таких значений:

$$\overline{v} = \{v_i\}, 1 \le i \le I. \tag{11}$$

Работу каждого нейрона первого слоя можно описать следующим образом:

$$x_{1,l} = \overline{v} \cdot \overline{net}_k \tag{12}$$

$$\overline{net}_k = \{\Delta_i\}, 1 \le i \le I, \tag{13}$$

$$\Delta_i = PRNG(IV) = \begin{cases} \Delta_i = 1, \text{электрод используется в нейроне} \\ \Delta_i = 0, \text{электрод не используется в нейроне} \end{cases}, \tag{14}$$

$$y_{1,l} = \frac{2}{1+e^{x_{1,l}}} - 1, \tag{15}$$

$$t_l = \mathrm{f}_1(y_{1,l}) = \begin{cases} 1, y_{1,l} \geq 0 \\ -1, y_{1,l} < 0 \end{cases}, 1 \leq l \leq L \ , \tag{16}$$

где $x_{1,k}$ – это результат работы сумматора нейрона l первого слоя; Δ_i – коэффициент использования данных электрода i в нейроне; $y_{1,l}$ – передаточная функция первого слоя нейронной сети; $\mathrm{f}_1(y_{1,l})$ – решающее правило для нейрона первого слоя.

Для обучения первого слоя нейронной сети целесообразно применять следующую величину:

$$Q(a_i) = \frac{\left| E_{Чужой}(a_i) - E_{Свой}(a_i) \right|}{\sigma_{Свой}(a_i)} \tag{17}$$

где E – среднее значение и σ - дисперсия биометрических данных.

Весовые коэффициенты для первого слоя рассчитываются следующим образом:

$$w_i = \frac{Q(a_i)}{\sigma_{Чужой}(a_i)}. \tag{18}$$

Знак весового коэффициента получаем на основе расчета разностей математического ожидания данных образов "Свой" и "Чужой":

$$sign(w_i) \begin{cases} sign(w_i) = sign\left(E_{Свой}(a_i) - E_{Чужой}(a_i)\right), y_{1,l} = 1 \\ sign(w_i) = -sign\left(E_{Свой}(a_i) - E_{Чужой}(a_i)\right), y_{1,l} = -1 \end{cases}. \tag{19}$$

Каждый нейрон второго слоя можно описать следующим образом:

$$x_{2,r} = \sum_{l=1}^{L} W_l t_l \Delta_r \ , 1 \leq l \leq L, \tag{20}$$

$$\Delta_r = PRNG(IV) = \begin{cases} \Delta_r = 1, \text{электрод используется в нейроне} \\ \Delta_r = 0, \text{электрод не используется в нейроне} \end{cases}, \tag{21}$$

$$y_{2,r} = \frac{2}{1+e^{x_{2,r}}} - 1 \tag{22}$$

$$k_r = \mathrm{f}_2(y_{2,r}) = \begin{cases} 1, y_{2,r} \geq 0 \\ 0, y_{2,r} < 0 \end{cases}, 1 \leq r \leq R \ , \tag{23}$$

где $x_{2,r}$ – это результат работы сумматора нейрона второго слоя; Δ_r – коэффициент использования компонента t_l в нейроне; $y_{2,r}$ – передаточная функция второго слоя нейронной сети; $\mathrm{f}_2(y_{2,r})$ – решающее правило для нейрона второго слоя.

Весовые коэффициенты рассчитываются для второго слоя нейронной сети по следующей формуле:

$$W_l = \frac{b\omega_l}{E(\omega_l)}, \tag{24}$$

где b – коэффициент стабилизации, экспериментально выбираемый для машинного обучения при разработке процедуры биометрической аутентификации, ω_i – индикатор стабильности i-го разряда выходов нейронов первого слоя:

$$\omega_i = 2 \cdot \left|0{,}5 - P_{0,i}\right| = 2 \cdot \left|0{,}5 - P_{1,i}\right|, \tag{25}$$

где $P_{0,i}$ – вероятность появления состояния «0» в i-м контролируемом выходе нейрона; $P_{1,i}$ – вероятность появления состояния «1» в i-м контролируемом выходе нейрона.

Для нейросетевого преобразователя рассчитываются следующие характеристики: неполнота базы естественных биометрических образов "Чужой" ϕ, математическое ожидание расстояния Хэмминга $\overline{H}(\overline{K}_{rest})$, среднее значение модулей коэффициентов парной корреляции r_{xy}, стабильность выходного кода $P_{0,i}$, $P_{1,i}$, вероятность ошибки первого рода P_1, вероятность ошибки второго рода P_1.

Введенные показатели позволяют оценить наличие свойств данной математической модели. В предыдущих работах были показаны наличие свойство полноты, адекватности, экономичности, наглядности. Частично установлена продуктивность математической модели [2,3]. Однако еще требуется установление свойств точности и робастности.

Список литературы

1. Маркелов Г.Е. Основные принципы построения математических моделей // Вестник МГТУ им. Н.Э. Баумана. Сер. Естественные науки, 2005.- № 4.- С. 59–70

2. Гончаров С.М., Боршевников А.Е. Построение нейросетевого преобразователя "Биометрия - код доступа" на основе параметров визуального вызванного потенциала электроэнцефалограммы / С.М. Гончаров, А.Е. Боршевников // Доклады Томского государственного университета систем управления и радиоэлектроники: Научный журнал. – Томск: Изд-во ТУСУР, 2014. – № 2. – С. 51–55.

3. Гончаров С.М. Восстановление секретного ключа на основе электроэнцефалограммы при движении глаз с закрытыми веками. / Гончаров С.М., Боршевников А.Е., Михайлов А.Г., Апальков А.Ю. // Журнал «Информация и безопасность». Том. 19, часть 1. Воронеж: ВГТУ, 2016. - С. 114-117.

УДК 004.78

Каменная Евгения Владимировна,
МГУ им. адм. Г.И.Невельского,
Jen_s07@mail.ru
Щербинина Инна Александровна,
к. пед. н., МГУ им. адм. Г.И.Невельского,
shcherbinina@msun.ru

ЛОКАЛИЗАЦИЯ И МАРШРУТИЗАЦИЯ В БЕСПРОВОДНЫХ ПОДВОДНЫХ СЕТЯХ, ИСПОЛЬЗУЕМЫХ ДЛЯ ОХРАНЫ МАРИФЕРМ

На сегодняшний день вопрос безопасности подводных объектов приобретает особую актуальность, поскольку охрана экосистем является одним из путей обеспечения их развития. В охране нуждаются такие акватории как, морские заповедники и заказники, марикультурные фермы, акватории портов. Террористические угрозы, кражи и хищения, природные катаклизмы и всевозможные чрезвычайные ситуации могут воздействовать на подводные структуры, такие как ГЭС, нефте- и газопроводы, нефтяные платформы, архитектурные элементы построек, плантации аквакультур.

Угроза кражи с плантаций может быть как внешняя, так и внутренняя. Внутренняя угроза может быть реализована сотрудниками фермы непосредственно при выполнении своих обязанностей (с прибрежной территории фермы). Внешняя угроза исходит от браконьеров, которые могут воспользоваться 2 способами:

– надводный (проплыть на плавсредстве на территорию фермы);

– подводный (использовать водолазное оборудование для проникновения на территорию фермы непосредственно в подводном пространстве).

Соответственно необходимо разработать комплексную систему охраны марикультурных ферм (рис. 1) , которая будет включать в себя: охрану по периметру наземной территории, охрану подводной границы морского хозяйства, охрану надводного пространства. Кроме того, требуется индивидуальный подход и предварительное обследование каждой отдельной плантации. При построении системы защиты важнейших объектов от подводных угроз задача раннего обнаружения цели является самой важной, но не единственной (Леонид М. Антокольский).

Среди гидроакустических станций (ГАС, сонары), предназначенных для защиты от подводных нарушителей следует отметить систему AquaShield, выпускаемую израильской фирмой DSIT и комплекс инженерно-технических средств физической защиты, производимый российской компанией ОАО «Тетис Про».

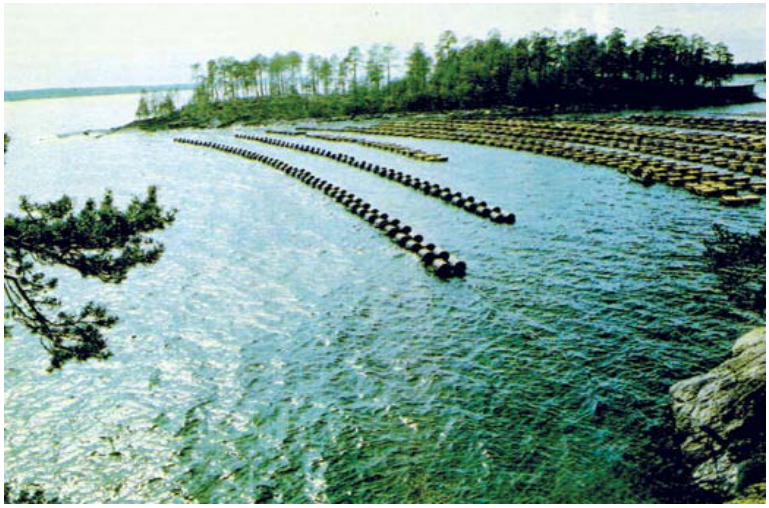

Рис. 1. Марикультурная ферма

Для того чтобы обеспечить безопасность подводного направления, комплекс физической защиты должен включать следующие системы:

– комплексы технических средств обнаружения и наблюдения;

– системы сбора и обработки информации;

– системы видеонаблюдения и контроля;

– системы протоколирования, видеоархивирования и хранения информации;

– локальные вычислительные сети;

– средства оповещения, тревожно-вызывную сигнализацию;

– средства воздействия на нарушителей;

– автоматизированные рабочие места операторов.

Для того чтобы обеспечить безопасность надводного пространства фермы, необходим комплекс мер по защите:

– радиолокационная станция (далее – РЛС) миллиметрового и сантиметрового диапазона для обнаружения мелких целей на близких расстояниях и крупных на больших;

– гидроакустическая система обнаружения подводного нарушителя на ближних (до 500 м) и дальних (до 1,5 км) расстояниях к объекту;

– система видеонаблюдения акватории с ZOOMом и системой видеоархивирования;

– сканирующие оптико-электронные системы видеонаблюдения акватории с тепловизионными устройствами.

Данные системы защиты крупномасштабны и дорогостоящи. Также они имеют определённые недостатки. Одним из них является необходимость в использовании ГАС большого радиуса действия, чтобы сотрудники безопасности имели достаточно времени для принятия адекватных мер, поскольку пловец может преодолеть расстояние в 200 метров за 3 минуты. Нарушители границы хозяйства должны быть не только обнаружены, но и классифицированы, так как всё большую популярность приобретает люби-

тельский дайвинг, морской туризм и нарушитель может быть случайным, оказавшимся в данном районе любителем.

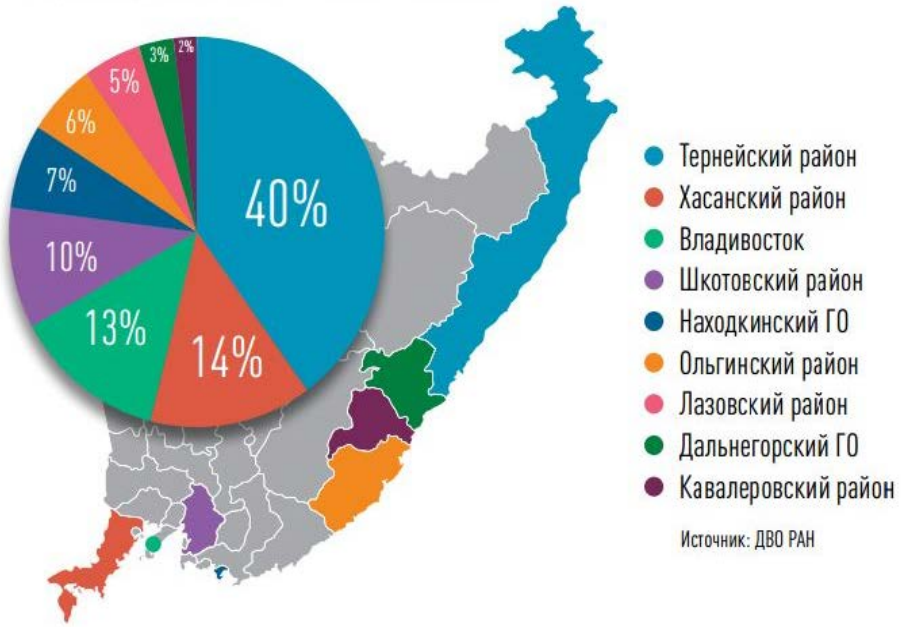

Рис. 2. Структура потенциальных ресурсов марикультуры в Приморском крае по районам

Создание подводных беспроводных сетей передачи информации является одним из актуальных направлений обеспечения безопасности труднодоступных объектов. В силу особенностей водной среды, организация подобных сетей требует разработки своих протоколов синхронизации, архитектур, алгоритмов обмена данными. Одной из первых является задача определения местоположения узлов сети относительно друг друга – латерация.

Наземные беспроводные коммуникационные сети передают данные с помощью радиоволн, излучаемых наземными антеннами и антеннами искусственных спутников. К сожалению, высокочастотные радиоволны совершенно не способны распространяться в водной среде. Поэтому большинство подводных беспроводных коммуникационных систем используют звуковые волны, которые достаточно хорошо распространяются в воде, беспрепятственно преодолевая большие расстояния. Такие акустические каналы используют сети датчиков, которые регистрирую возникновение и приближение цунами. Эти датчики с помощью звуковых сигналов передают данные оборудованию бакена, который находится на поверхности океана и который передаёт эти данные на спутник уже с помощью радиоволн. Несмотря на то, что множество подводных коммуникационных систем во всех уголках земного шара используют принципы подобные вышеописанному, их интеграция в одну единую систему является затруднительной, так как каждая из существующих систем имеет свою инфраструктуру и свои протоколы обмена информацией. Основной задачей в этом направлении является разработка и создание новых протоколов обмена в среде «вода-

вода» и «вода-воздух». Использование сетевых технологий сбора и передачи информации для объектов, находящихся в «воздушной» среде – общепринятая практика, которая, к сожалению, не может быть перенесена в «водную» среду. Создание подводных беспроводных сетей сопряжено с рядом серьёзнейших технологических трудностей, обусловленных глобальным различием свойств водной и воздушной среды. Использование «беспилотных» подводных аппаратов может стать не менее значимым, чем использование таких аппаратов в воздушной среде. Для этого необходимо в первую очередь обеспечить возможность связи между элементами сети мониторинга подводного пространства. Подводные сети нуждаются в разработке новых доступов к носителям информации, новых типов соединения, транспортировки и локализации отдельных узлов сети, собственных протоколов синхронизации и архитектурах. Одной из значимых задач является задача определение местоположения узлов сети относительно друг друга – задача локализации. Данные локализации необходимы для протоколов маршрутизации и доступа к данным. Первыми шагами в направлении унификации и глобализации системы подводных коммуникаций является работа исследователей из университета Буффало в Нью-Йорке, которые создали универсальные аппаратные средства и разработали протоколы связи общего применения, которые можно использовать для обеспечения надёжной связи под водой на больших дистанциях (Томмазо Мелодия (Tommaso Melodia), профессор университета Буффало).

Для определения координат подводных объектов с помощью гидроакустики, применяются три вида систем, отличающиеся между собой размерами базовых линий сети, т.е. расстояний между узлами:

– системы со сверхкороткой базой, являются угломерными системами, в которых направление на объект определяется путём измерения разности фаз между узлами сети, установленными на расстоянии друг от друга менее 10 м, имеют ограниченную точность определения координат и высокий уровень помех;

– системы с короткой базой являются разностно-дальномерными системами, в которых координаты подводного объекта вычисляются по разности времен прихода (ToA) импульсов, излучаемых узлом-передатчиком с подводного объекта на три гидроакустических узла-приёмника, расположенных под водой и образующих две пересекающиеся базы; точность определения координат зависит от длины базы, которая для систем с короткой базой составляет около 20 м, имеют невысокую помехозащищённость, являются дорогостоящими;

– системы с длинной базой являются дальномерным системами, местоположение подводного объекта вычисляется по времени прихода сигнала; временные интервалы прохождения сигнала измеряются в абсолютных значениях установленного времени и пересчитываются в расстояния с учётом скорости звука в воде; по результатам измерения расстояний между подводным объектом и минимум тремя стационарными узлами-

передатчиками (маяками), установленными в различных точках морского дна в нескольких километрах друг от друга MLC рассчитывает местоположение с помощью триангуляционного алгоритма; точность позиционирования в центре ограничена.

В настоящее время для мониторинга и удалённого контроля автономных подводных аппаратов (далее – АПА) в различных точках поверхности моря устанавливаются дрейфующие буи, образующие длинную базу. Каждый буй оборудован навигационным приёмником глобальной системы позиционирования (GPS), часами, синхронизированными с часами GPS, гидроакустической приёмной системой с подводным преобразователем и радиомодемом. Такие буи получили название GIB-буи. Каждый буй измеряет собственные координаты и время запаздывания, и в установленные моменты времени передаёт эти данные по радиоканалу через радиомодем на судно сопровождения или береговую управляющую станцию. Гидроакустический передатчик подводного объекта периодически излучает сигнал в установленные моменты времени. С учётом скорости звука в воде, по разности времени прихода сигналов вычисляются расстояния от подводного объекта до каждого из буев, а далее отображаются координаты подводного объекта и координаты всех буев [1].

Методы локализации в ПАСС можно классифицировать по двум категориям:

– централизованные методы – текущие координаты каждого объекта в сети вычисляются в центре управления (береговом или на обеспечивающем судне); применяются для пошагового определения местоположения узлов;

– распределённые методы – каждый сенсорный узел рассчитывает своё местоположение самостоятельно.

Централизованные и распределённые методы подразделяются на схемы, основанные на оценочном и прогнозируемом подходе. При оценочном подходе вычисляется необходимая информация о текущем местоположении сенсорного узла. В то время как при прогнозируемом подходе вычисляется будущее интересуемое положение сенсорного узла, которое с определенной вероятностью определяется при измерениях расстояний, предыдущей и текущей локализации и местонахождении привязок. Прогнозируемый подход используется в мобильных и гибридных подводных сетях.

Централизованные методы локализации:

– метод автолокализации при известном маршруте;
– локализация по областям;
– гиперболический метод определения локализации;
– трёхмерная мультимощная локализация по областям;
– пассивная локализация с использованием магнитометра.

К распределённым методам относятся:

– локализация с помощью подводных аппаратов;
– протокол локализации погружения и подъёма;
– многоступенчатая локализация;
– протокол крупномасштабной иерархической локализации;
– протокол локализации с помощью съёмного подъёмника для трансивера / приёмапередатчика;
– трёхмерная подводная локализация;
– локализация без привязок;
– схема подводного позиционирования;
– схема крупномасштабной локализации;
– масштабируемая локализация с прогнозом мобильности.

В большинстве протоколов локализации подразумевается, что процесс локализации функционирует отдельно от других задач системы. Выбор режима работы ПАСС, правильно подобранный уровень параллельного функционирования системы для мониторинговых измерений и позиционирования позволяет повысить эффективность ПАСС, экономить энергию блоков питания сенсоров. Для процедуры выбора привязочных узлов и узлов-ссылок необходимо использовать информацию о параметрах акустического канала и о качестве связи, что повысит точность измерения расстояний и существенно улучшит оценку локализации.

Беспроводные сенсорные сети (далее – БСС) – новое перспективное направление в области систем передачи и сбора данных. Беспроводная сенсорная сеть представляет собой распределенную, самоорганизующуюся и устойчивую к отказу сеть миниатюрных электронных устройств, обменивающихся информацией по беспроводному каналу связи. Предполагается, что такие сети будут иметь многоячейковую (mesh) топологию и состоять из большого числа (до нескольких десятков тысяч) узлов, которые способны ретранслировать сообщения друг друга.

Маршрутизация пакетов является одной из наиболее актуальных задач в области БСС, так как характеристики протокола маршрутизации оказывают существенное влияние на энергопотребление, пропускную способность и другие показатели качества обслуживания сети. Из-за особенностей БСС применение в них традиционных алгоритмов маршрутизации, разработанных для беспроводных эпизодических сетей, нецелесообразно.

Значительную роль в работе беспроводных сетей отведена протоколам маршрутизации. Они помогают осуществлять самоорганизацию узлов и доставку пакетов оптимальными маршрутами в соответствии с алгоритмами, перечисленными в используемом в сети протоколе. С помощью протоколов маршрутизации оптимизируется использование ресурсов сети, таких как расход энергии, использование процессорного времени, памяти и др. А это значит, что применение эффективных протоколов маршрутизации позволяет максимизировать время жизни сети [2].

Протоколы маршрутизации, используемые для мобильных самоорганизующихся сетей, подразделяются на четыре основные группы:

– протоколы с проактивной маршрутизацией,
– протоколы с реактивной маршрутизацией,
– гибридные протоколы,
– протоколы, использующие данные о географическом положении узлов.

Перспективой развития методов локализации в ПАСС являются протоколы географической маршрутизации. Один из наиболее используемых протоколов географической маршрутизации – LAR (рис. 3). Данный протокол использует информацию о местоположении узла-источника для ограничения области (зоны запроса), где производится поиск маршрута. В итоге количество сообщений о запросе искомого маршрута сокращается.

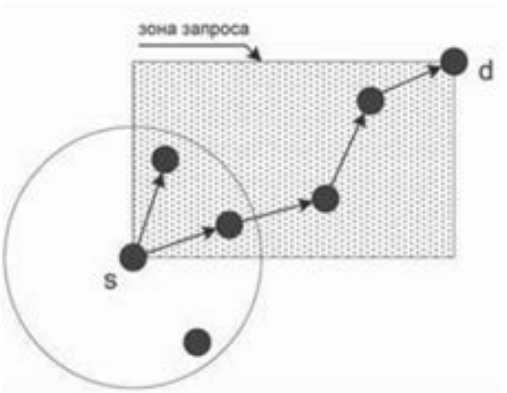

Рис. 3. Принцип маршрутизации LAR

Однако, использование разработанных алгоритмов вычисления географических координат требует точной информации о местоположении узлов сети, что затруднено при организации подводной сети. Альтернативой может стать метод распознавания и кластеризации подводных объектов. Кластеризация – задача машинного обучения, состоящая в разбиении заданной выборки объектов (данных) на непересекающиеся подмножества/группы (кластеры) на основе близости их признаков/значений. Таким образом, каждый кластер состоит из схожих объектов.

Кластеризация позволяет:

– лучше понять данные (выявив структурные группы);
– компактно сохранить данные;
– выявить новые объекты.

Выделяют две основные классификации алгоритмов кластеризации: иерархические и плоские.

Иерархические алгоритмы (также называемые алгоритмами таксономии) строят не одно разбиение выборки на непересекающиеся кластеры, а систему вложенных разбиений. Таким образом, на выходе мы получаем

дерево кластеров, корнем которого является вся выборка, а листьями – наиболее мелкими кластерами.

Плоские алгоритмы строят одно разбиение объектов на кластеры: чёткие и нечёткие.

Чёткие (или непересекающиеся) алгоритмы каждому объекту выборки ставят в соответствие номер кластера, т.е. каждый объект принадлежит только одному кластеру. Нечёткие (или пересекающиеся) алгоритмы каждому объекту ставят в соответствие набор вещественных значений, показывающих степень отношения объекта к кластерам. Т.е. каждый объект относится к каждому кластеру с некоторой вероятностью. В OpenCV, алгоритм k-means реализован в cxcore, т.к. он был реализован задолго до появления библиотеки ML.

Таблица 1

Алгоритмы кластеризации

Алгоритм кластеризации	**Форма кластеров**	**Входные данные**	**Результаты**
Иерархический	Произвольная	Число кластеров или порог расстояния для усечения иерархии	Бинарное дерево кластеров
k-средних	Гиперсфера	Число кластеров	Центры кластеров
c-средних	Гиперсфера	Число кластеров, степень нечеткости	Центры кластеров, матрица принадлежности
Выделение связных компонент	Произвольная	Порог расстояния R	Древовидная структура кластеров
Минимальное покрывающее дерево	Произвольная	Число кластеров или порог расстояния для удаления ребер	Древовидная структура кластеров
Послойная кластеризация	Произвольная	Последовательность порогов расстояния	Древовидная структура кластеров с разными уровнями иерархии

Развитие и совершенствование технологий, используемых в системах передачи данных определило появление нового класса телекоммуникационных сетей, получивших наименование ad hoc-сети (от лат. – *для данного случая*). Характерной особенностью этих сетей является динамическая, не имеющая постоянной структуры переменная топология, формируемая на базе автономных узлов, функционирующих в качестве маршрутизаторов и объединённых в коммуникационную самоорганизующуюся сеть, представляемую в виде произвольного графа.

Одним из видов ad hoc-сетей являются мобильные ad hoc-сети (MANETmobile ad hoc networks) – одноранговые самоорганизующиеся беспро-

водные сети с переменной топологией и отсутствием четкой инфраструктуры, предназначенные для связи между подвижными объектами [3]. В MANET-сети (рис. 4) каждый узел может независимо перемещаться в произвольном направлении вследствие чего изменения в топологии сети должны быть переданы другим узлам для поддержания правильной маршрутизации. Например, когда узел MH2 вследствие перемещения изменяет своё соединение с MH3 на соединение с узлом MH4, другие узлы сети должны получить информацию о новом маршруте от источника до пункта назначения через промежуточные узлы для пересылки пакетов между MH2 и MH3.

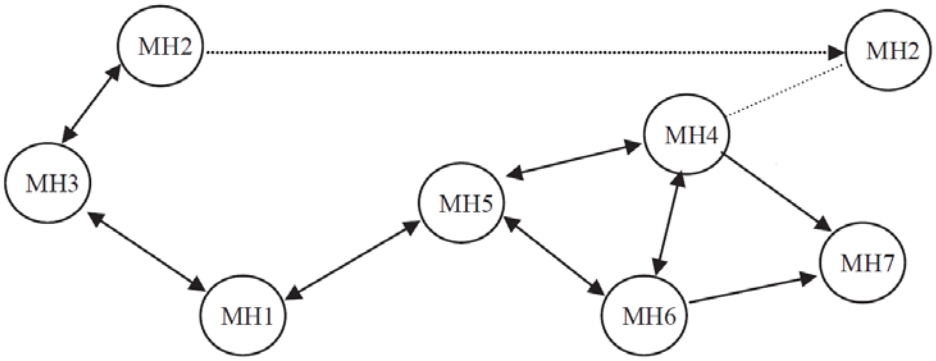

Рис. 4. Типовая MANET-сеть

Особый интерес в связи с простотой доступа в настоящее время к глобальным системам позиционирования (*GPS*, ГЛОНАС) представляют протоколы маршрутизации, в *MANET*- сетях использующие информацию о местоположении узлов для ограничения области отправки запросов. Эти протоколы (*Location-aware protocols)* предусматривают получение координат адресатов, а также некоторой информации о их передвижении:

– протокол LAR (Location-Aided Routing) на основе информации о месте расположения адресата и данных о направление и скорость движения узла-получателя отправляет пакеты к узлам только в «ожидаемой зоне» адресата, что уменьшает нагрузку от служебного трафика; в случае отсутствия у отправителя данной информации он рассматривает всю сеть как «ожидаемую зону» и инициирует служебную рассылку, расширяя зону запроса до достижения узлов, способных передать пакет адресату с использованием алгоритма широковещательной рассылки; помимо уменьшения объёма служебного трафика протокол LAR обеспечивает максимальную связности сети;

– протокол DREAM (Distance Routing Effect Algorithm for Mobility), использующий GPS координаты узлов включает проактивные и реактивные механизмы формирования маршрутов; в нём используется зависимость периода обновления таблиц маршрутизации от расстояния между узлами; так как удалённые узлы движутся относительно друг друга медленнее, чем близко расположенные, более редкое обновление таблиц мало влияет на точность маршрутизации; помимо этого в DREAM каждый узел

отправляет служебные пакеты, основываясь только на своей скорости перемещения, что значительно уменьшает загрузку сети служебным трафиком; использование DREAM обеспечивает выигрыш в пропускной способности и в энергетических показателях сети по сравнению с другими реактивными протоколами, так как данный протокол не имеет задержек на открытие маршрута.

Приведённые механизмы формирования маршрутов и функциональные возможности рассмотренных протоколов позволяют оптимизировать выбор протокола маршрутизации при проектировании MANET-сетей с учётом используемых сетевых технологий и заданных потребительских характеристик.

Список литературы

1. «A Survey of Architectures and Localization Techniques for Underwater Acoustic Sensor Networks» Melike Erol-Kantarci, Hussein T. Mouftah, and Sema Oktug, IEEE communications surveys & tutorials, vol. 13, no. 3, third quarter 2011

2. Павлов А.А., Датьев И.О. Протоколы маршрутизации в беспроводных сетях / А.А. Павлов, И.О. Датьев// Труды Кольского научного центра РАН. – 2014. – Информационные технологии № 5. – С. 64-75.

3. Орлов В.Г., Фадеев А.Н. Протоколы маршрутизации в мобильных ad-hoc- сетях //Материалы Международной научно-технической конференции, INTERMATIC, часть 6 / Московский технический университет связи и информатики.- МОСКВА 2012. –С. 208-212.

УДК 004.942

Касьянова Елена Владимировна

Магистр 2-го года обучения, кафедра автоматизации и управления, ДВФУ

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ТЕПЛОВОГО НАСОСА И ЕЁ РЕАЛИЗАЦИЯ В СРЕДЕ MATLAB

Развитие энергосберегающих технологий представляет собой перспективное направление, решаемое мировым сообществом в настоящее время. При этом достигаются следующие цели – сохранение невозобновляемых энергоресурсов и сокращение вредных выбросов в атмосферу продуктов сгорания.

Одним из решений указанной проблемы является использование энергосберегающих технологий на основе применения тепловых насосов (ТН). ТН находят применение для теплоснабжения и горячего водоснабжения жилых, административных, производственных зданий, обеспечения тепловой энергией технологических процессов.

Для оценки целесообразности применения теплонасосных технологий необходимо сравнение энергетической и экономической эффективности традиционных генераторов тепла и ТН различных типов.

В основе оценочного подхода лежит принцип моделирования и сравнения результатов. Существующие пакеты моделирования динамических систем, такие как Femlab, Matlab/Simulink используются для создания систем управления ТН на базе математических моделей [2, 3]. В [3, 4] приведена математическая модель ТН:

$$\begin{aligned} &COP = k \cdot \frac{0.5 \cdot T_{cin} + 0.5 \cdot T_{cout} + 273.15}{\left(0.5 \cdot T_{cin} + 0.5 \cdot T_{cout}\right) - \left(0.5 \cdot T_{vin} + 0.5 \cdot T_{vout}\right)} \\ &\frac{dT_{cout}}{dt} \frac{1}{C_c} \cdot \left[F_{cin} \cdot cw \cdot \left(T_{cin} - T_{cout}\right) + COP \cdot Ehp\right] \\ &\frac{dT_{vout}}{dt} \frac{1}{C_v} \cdot \left[F_{vin} \cdot cw \cdot \left(T_{vin} - T_{vout}\right) + \left(COP - 1\right) \cdot Ehp\right] \end{aligned} \quad (1),$$

где $T, °C$ - температура, COP - коэффициент производительности, k - коэффициент эффективности теплового насоса, $C, Дж/К$ - теплоемкость теплоносителя и труб в тепловом насосе, $F, кг/сек$ - массовый поток, $Ehp, Вт$ - мощность электропитания теплового насоса, $cw, Дж/К$ - теплоемкость воды. Нижние индексы: «c» - теплоноситель в конденсаторе, «v» - теплоноситель в испарителе, «in» - входной поток, «out» - выходной поток.

Рассмотрим принцип построения динамической модели в Matlab/Simulink с использованием Simulink-функции (S-функции). Несмотря на то, что набор стандартных блоков Simulink достаточно обширен, в практике моделирования встречаются ситуации, когда нужного блока нет, либо использование структурного подхода делает модель слишком сложной. В этом случае рекомендуется использовать технологию S-функций для создания блока. С помощью языков программирования (Matlab, C, C++ и др.) пользователь может создать описание сложного блока и подключить его к Simulink-модели. Создаваемые блоки могут быть непрерывными, дискретными или гибридными.

Каждая задача при вызове S-функции в процессе моделирования решается с помощью внутренней функции (callback-метода). В Matlab S-функции используют следующие методы:

1. mdlInitializesizes – Инициализация, в начале моделирования Simulink инициализирует S-функцию, при этом устанавливается количество и размерность входных и выходных портов, задается шаг модельного времени для блока, выделяется память для хранения переменных и устанавливает размерность массивов.
2. mdlOutputs – Вычисление значений выходных сигналов на внешнем шаге моделирования, рассчитанные выходные сигналы блока передаются на его выходные порты.
3. mdlUpdate – Расчет дискретных переменных состояния на внешнем шаге моделирования. Дискретные переменные состояния сохраняют свое значение до следующего цикла моделирования.
4. mdlDerivatives – Расчет производных переменных состояния.
5. mdlTerminate – Завершение работы S-функции.

Если S-функция содержит непрерывные переменные состояния, Simulink вызывает callback-методы mdlDerivatives и mdlOutputs для расчета производных переменных состояния и выходных переменных на внутренних шагах моделирования.

Вызов каждого из методов Simulink задает с помощью переменной flag, являющейся входным параметром S-функции [5 - 7].

Рассмотрим реализацию S-функции, описывающей функционирование теплового насоса в среде Matlab/Simulink. В таблице 1 приведены обозначения переменных модели, на рисунке 1 приведено окно настроек блока S-функции в среде Matlab/Simulink и подсистема блока. Ниже приведен листинг модуля S-функции hpmodel, реализующей динамическую модель теплового насоса (1).

Таблица 1

Обозначение переменных модели

Переменная	**Вход (u) / Выход(y)**	**Описание**
Tvin	u(1)	Температура входного потока теплоносителя в испарителе [°, C]
Fvin	u(2)	Массовый входной поток в испарителе [кг/сек]
Tcin	u(3)	Температура входного потока теплоносителя в конденсаторе [°, C]
Fcin	u(4)	Массовый входной поток в конденсаторе [кг/сек]
Ehp	u(5)	Мощность электроустановки [Вт]
Tvout	y(1)	Температура выходного потока теплоносителя из испарителя [°, C]
Tcout	y(2)	Температура выходного потока теплоносителя из конденсатора [°, C]
COP	y(3)	коэффициент производительности [-]

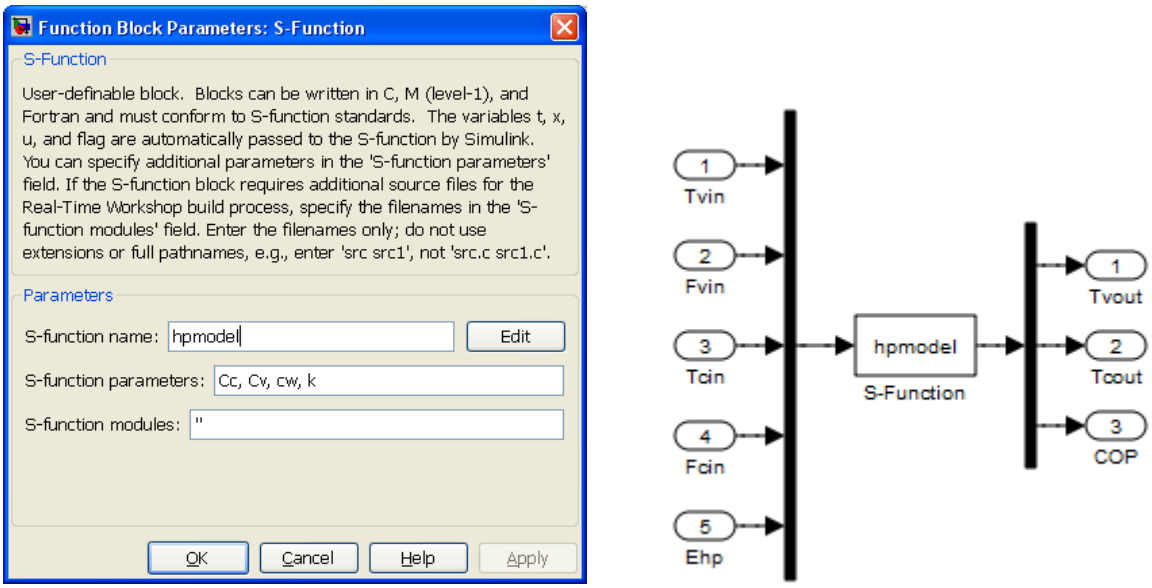

Рис. 1. Реализация S-функции в среде Matlab/Simulink

Листинг 1. Модуль S-функции

```
function [sys, x0, str, ts] = hpmodel(t, x, u, flag, Cc, Cv, cw, k)
switch flag,
    case 0,
        [sys, x0, str, ts] = mdlInitializeSizes;
    case 1,
        sys = mdlDerivatives(t, x, u, Cc, Cv, cw, k);
    case 3,
        sys = mdlOutputs(t, x, u);
    case { 2, 4, 9 },
        sys = [];
    otherwise
    error(['Unhandled flag = ',num2str(flag)]);
end

function [sys, x0, str, ts] = mdlInitializeSizes
global COP, COP = 0;
sizes = simsizes;
sizes.NumContStates = 2; % непрерывные
sizes.NumDiscStates = 0; % дискретные
sizes.NumOutputs = 3;    % выходы
sizes.NumInputs = 6;     % входы
sizes.DirFeedthrough = 0;
sizes.NumSampleTimes = 1;
sys = simsizes(sizes);
x0 = [10; 12];           % начальные условия
str = [];
ts  = [0 0];
% Окончание mdlInitializeSizes

function sys = mdlDerivatives(t, x, u, Cc, Cv, cw, k)
global COP;
Tvm = (u(1) + x(1))/2;
Tcm = (u(3) + x(2))/2;
COP = k*(273.15 + Tcm)/(Tcm - Tvm);
sys = [(1/Cv)*(u(2)*cw*(u(1) - x(1)) - (COP - 1)*u(5));
       (1/Cc)*(u(4)*cw*(u(3) - x(2)) + COP*u(5))];
% Окончание mdlDerivatives

function sys = mdlOutputs(t, x, u)
global COP;
sys = [x(1); x(2); COP];
```

Для использования модели в среде Matlab/Simulink необходимо задаться параметрами, характеризующими теплоемкости теплоносителей испарителя и конденсатора. Также некоторые неизвестные коэффициенты могут быть получены путем идентификации по экспериментальным данным.

Список литературы

1. Калнинь И.М., Савицкий И.К Тепловые насосы: вчера, сегодня, завтра. Холодильная техника 2000, №10, 6с.

2. A.W.M. (Jos) van Schijndel, Integrated building physics simulation with Femlab/Simulink/Matlab, Eighth International IBPSA Conference, Eindhoven, Netherlands.August 11-14, 2003

3. Schijndel, A.W.M. van & Wit, M.H. de , Advanced simulation of building systems and control with SimuLink, 8TH IBPSA Conference Eindhoven. August 11-14. pp. 1185-1192.

4. Application of HAMLab for Whole Building HAM Response Modeling, A.W.M. (Jos) van Schijndel, Eindhoven University of Technology.

5. Дьяконов В., Круглов В. MATLAB. Анализ, идентификация и моделирование систем. Специальный справочник. – СПб.: Питер, 2002. – 448с.

6. Дьяконов В. П. MATLAB 6.5 SP1/7 + Simulink 5/6 ©. Основы применения. Серия «Библиотека профессионала». – М.: СОЛОН-Пресс, 2005. – 800с.: ил.

7. Черных И.В. SIMULINK: среда создания инженерных приложений / Под общ. ред к.т.н. В.Г. Потёмкина. – М.: ДИАЛОГ-МИФИ, 2003. –496с.

УДК 004.942

Касьянова Елена Владимировна

Магистр 2-го года обучения, кафедра автоматизации и управления, ДВФУ

ОБЗОР МЕТОДОВ ИДЕНТИФИКАЦИИ ДИНАМИЧЕСКИХ ОБЪЕКТОВ

Синтез системы управления сложной динамической системой, такой как система теплоснабжения, основан на использовании математической модели управляемого объекта. Ключевым объектом такой системы является тепловой насос. Известные математические модели данного объекта представляют собой систему дифференциальных уравнений с параметрами, зависящими от конкретной модели [1]. Задачей идентификации является определение этих параметров.

Задача идентификации формулируется следующим образом: по результатам наблюдений за входными и выходными переменными исследуемого объекта необходимо построить оптимальную в некотором смысле его модель. При этом объект находится в нормальном режиме функционирования (т. е. в обстановке случайных возмущений и помех) [2-4].

В современной теории систем автоматического управления развиваются специальные методы идентификации динамических объектов управления в режиме нормальной эксплуатации (т.е. в обстановке случайных возмущений и помех). Именно к этим методам вначале был применён термин «идентификация».

В соответствии с современной теорией можно предложить следующую классификацию методов идентификации:

1) по конечному результату идентификации:

– структурная, когда определяется (или задается) структура уравнений модели;

– параметрическая, когда при известной структуре уравнений определяют неизвестные параметры;

2) по способу изучения объекта идентификации:

– активная, когда объект исследуется вне контура управления, как правило, в лабораторных условиях;

– пассивная, когда объект функционирует в контуре управления, находится в процессе нормальной эксплуатации;

3) по типу идентифицируемой модели:

– линейная и нелинейная;

– детерминированная и стохастическая;

– с непрерывным и дискретным временем;

– стационарная и нестационарная;

– одномерная и многомерная;

– статическая и динамическая;

– с сосредоточенными и распределёнными параметрами.

Использование модели для решения задач синтеза системы управления требует проверку адекватности модели и объекта. Адекватность предполагает воспроизведение моделью с необходимой полнотой всех свойств объекта, существенных для целей данного исследования.

Таким образом, задача идентификации может быть представлена в виде совокупности подзадач, таких как выбор структуры модели, оценка параметров и проверка адекватности модели.

Список литературы

1. A.W.M. (Jos) van Schijndel, Integrated building physics simulation with Femlab/Simulink/Matlab, Eighth International IBPSA Conference, Eindhoven, Netherlands.August 11-14, 2003

2. Дьяконов В., Круглов В. MATLAB. Анализ, идентификация и моделирование систем. Специальный справочник. – СПб.: Питер, 2002. – 448с.

3. Мирошник И.В., Никифиров В.О., Фрадков А.Л. Нелинейное и адаптивное управление сложными динамическими системами. СПб.: Наука, 2000.

4. Дейч А.М. Методы идентификации динамических объектов. М.: Энергия, 1979.

УДК 62-97/-98

Клименко Сергей Александрович
Магистр 2-го года обучения, кафедра автоматизации и управления, ДВФУ

РАЗРАБОТКА СТЕНДА НА БАЗЕ МИКРОКОНТРОЛЛЕРА ARDUINO MEGA2560 ДЛЯ ИССЛЕДОВАНИЯ ХАРАКТЕРИСТИК ВЫСОКОВОЛЬТНЫХ БАТАРЕИ ГИБРИДНОГО АВТОМОБИЛЯ

В последнее время большую популярность стали набирать гибридные автомобили. Автомобилисты стали покупать автомобиль, использующий одновременно и электрический, и традиционный двигатель внутреннего сгорания – это автомобили с гибридным двигателем. Выбор гибридного автомобиля обусловлен не только более экономическим расходом топлива, но и наименьшим выбросом загрязняющих веществ в окружающую среду, которые вредят экологии.

Одна из составных частей гибридного автомобиля – это высоковольтная батарея (далее – ВВБ). Ее задача – это накапливание «лишней» энергии. Она накапливается при движении автомобиля выше 50 км/ч или при торможении [2]. Выделение накопленной энергии происходит к примеру, когда необходимо прогреть ДВС, салон или при движении автомобиля с малой скоростью.

ВВБ гибридного автомобиля, как и любой аккумулятор имеет определенный срок службы и определенное количество циклов заряд – разряд, после которого ухудшаются характеристики аккумулятора. Производителем автомобиля предусмотрена встроенная система для мониторинга высоковольтной батареи. Информация по батареи отображается на дисплее, расположенного на приборной панели внутри салона автомобиля. Состояние батареи всегда находится перед глазами автовладельца. Но настает время, когда необходимо заменить высоковольтную батарею.

Существующее решение задачи

Производителями гибридного автомобиля уже предусмотрена встроенная система для мониторинга состояния высоковольтной батареи. Когда характеристики батареи не соответствуют номинальным значениям, на приборной панели автомобиля появляется значок ошибки, означающий неисправность высоковольтной батареи. Необходимо обратиться в сервисы, специализирующиеся по ремонту высоковольтных батарей гибридных автомобилей. Так как ВВБ состоит из отдельных модулей, то из строя могут выйти один или несколько модулей. Рекомендуется менять отдельно модули, если из общего количество модулей выходит из строя 2 – 3 модуля.

Например, напряжения на паре модулей ВВБ автомобиля марки Toyota Prius-20 NHW20 равно 14.4 В [3]. Номинальное общее напряжение всей батареи составляет 274.4 В. Если при проверки пары модулей, напряжение на нем не соответствует номинальному, то необходимо заменить неисправный модуль. После замены модулей необходимо проверить напряжение на модулях. Один автомеханик садится за руль автомобиля и ездит на машине в течении часа, второй садится рядом с высоковольтной батареей и измеряет напряжение на парах модуля. Если после замены модулей, напряжение на всех парах модулей высоковольтной батареи соответствует номинальному, то заменен неисправный модуль. Алгоритм по замене модуля ВВБ повторяется, до тех пор, пока напряжение на парах модулей и общее напряжение всей батареи не будет соответствовать номинальному значению напряжения.

Исследование и построение решения задачи

Моим объектом исследования стал метод замены и исследования характеристик высоковольтной батареи гибридного автомобиля.

Встроенная система для измерения характеристик модулей ВВБ не способна предоставить полную информацию автовладельцу по состоянию батареи и не позволяет проверить состояние купленной батареи, не выполнив перед этим непосредственно установку ее в машину. Так же система зарядки HV Battery устроена таким образом, что система не может определить точный номер «недозаряда» конкретного модуля. Когда один модуль выходит из строя («просела» до минимального уровня), то система, не обращая внимания на то, что заряд идет на всю высоковольтную батарею, что приводит к перегреву и к перезаряду, что может привести к разрушению батареи. В связи затраты большого количества времени на демонтаж и монтаж ВВБ, появилась идея о создании стенда, который позволит избегать лишние затраты времени на демонтаж и монтаж высоковольтной батареи, а также расширит количество исследуемых параметров батареи.

Одно из главных преимуществ стенда – это его универсальность. Использование стенда для измерения характеристики ВВБ любой марки автомобиля.

Описание стенда

Для стенда был выбран контроллер Arduino Mega2560 компании Arduino Software [1]. Этот контроллер имеют ряд преимуществ:

1. Низкая стоимость.

2. Кросс платформенность – способность программного обеспечения функционировать в нескольких различных операционных системах или на разных аппаратных платформах.

Стенд находиться на этапе разработки. На рисунке 1 представлена структурная схема работы стенда.

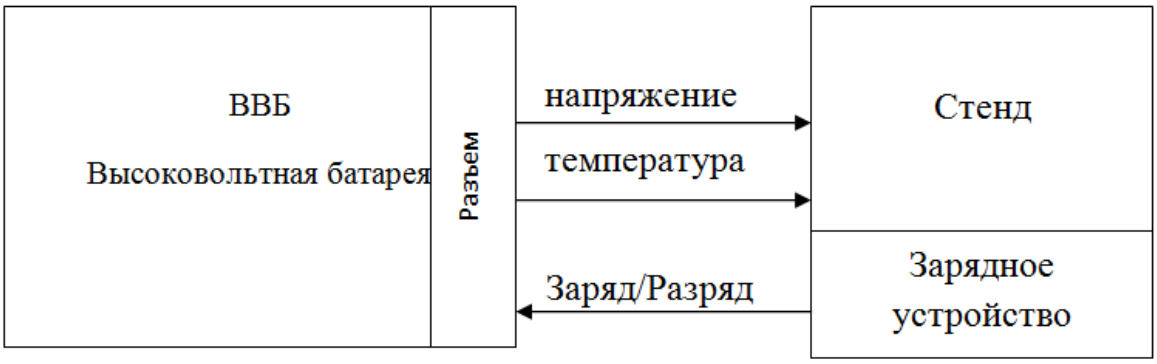

Рис. 1. Структурная схема стенда

Список литературы

1. Материалы по программированию Arduino. [Электронный ресурс] Режим доступа: http://arduino.ru. Дата обращения 19.04.2017г.
2. Сообщество машин и людей. [Электронный ресурс] Режим доступа: https://www.drive2.ru. Дата обращения 19.04.2017г.
3. Сайт автовладельцев. [Электронный ресурс] Режим доступа: http://www.drom.ru. Дата обращения 19.04.2017г.

УДК 62-97/-98

Клименко Сергей Александрович

Магистр 2-го года обучения, кафедра автоматизации и управления, ДВФУ

ОБЗОР ПРОГРАММИРУЕМОГО ЛОГИЧЕСКОГО КОНТРОЛЛЕРА КОМПАНИИ «ОВЕН» ПЛК 110/ ПЛК 160

Компания «Овен» – ведущий российский разработчик и производитель контрольно-измерительных приборов и средств автоматизации для различных отраслей промышленности. Компания работает с 1991 года. За 25 лет тысячи предприятий автоматизировали свои технологические процессы, используя компоненты автоматики ОВЕН. Продукция ОВЕН применяется в машиностроении и металлургии, химических и нефтехимических производствах, строительной и деревообрабатывающей отраслях, пищевой и упаковочной промышленностях, медицине, энергетике, ЖКХ, сельском хозяйстве и других сферах [1].

Качество программируемых логических контроллеров (ПЛК) компании ОВЕН, не отстает от продукции выпускаемыми мировыми гигантами по производству ПЛК и автоматики. Контроллеры серии ПЛК 110/ ПЛК 160 подходят для систем автоматизации среднего уровня и распределенных систем управления. Использование во многих сферах производства: в системах HVAC, в сфере ЖКХ (ИТП, ЦТП), в АСУ водоканалов (водопод-

готовка, насосные станции), для управления малыми станками и механизмами, для управления пищеперерабатывающими и упаковочными аппаратами, для управления климатическим оборудованием, для автоматизации торгового оборудования, в сфере производства строительных материалов, делает эти контроллеры универсальными в использовании.

Таблица 1

Сравнительная таблица контроллеров ОВЕН ПЛК110/160

Контроллер	Дискретные входы	Дискретные выходы	Аналоговые входы	Аналоговые выходы	RS-485
ПЛК110-30	18	12	нет	нет	2 шт.
ПЛК110-32	18	14	нет	нет	1 шт.
ПЛК110-60	36	24	нет	нет	2 шт.
ПЛК160	16	12	8	4	1 шт.

Серия ПЛК 110-30/32/60 отличается между собой количеством дискретных входов, выходов на контроллере, без аналоговых входов, выходов. Если в системе необходимо произвести измерения аналоговых величин, то отдельно заказывается аналоговый модуль, который по протоколу ModBus обменивается данными с ПЛК. В ПЛК160 имеется ввод и вывод аналогового сигнала в контроллер, но имеет самое маленькое количество дискретных входов, выходов.

Так же компания обновляет линейки контроллеров, модернизирует внутреннюю комплектацию и вносит изменения в модель корпуса для более удобного пользования или монтажа.

Таблица 2

Таблица сравнение ПЛК110 (выпускаемого ранее) и ПЛК110[М02] (модернизированного)

Параметр	ПЛК110	ПЛК110[М02]
Вычислительный ресурс		
Процессор	200 Мгц	400 Мгц
ОЗУ	8 МБ	16 МБ
ПЗУ	8 МБ	6 МБ
Операционная система	нет	Есть, EmbOS Segger
Интерфейсы	RS-232	RS-232
	RS-232 Debug	RS-232 Debug
	RS-485	RS-485
	Ethernet	Ethernet
	USB Device	USB Device
		USB HOST
Работа по беспроводным сетям	SMS, CSD	SMS, CSD, GPRS
Питание 5В в RS-232	нет	Есть
Ведение архивов на USB Flash	нет	До 8 ГБ
Быстрые входы	Есть, до 10 кГц	Есть, до 100 кГц
Быстрые выходы	до 5 кГц	До 100 кГц

Программирование контроллеров осуществляется в среде разработки CODESYS v.2.3.x [2], максимально соответствующей стандарту МЭК 61131:

– поддержка 5 языков программирования;

– мощное средство разработки и отладки комплексных проектов автоматизации на базе контроллеров;

– количество логических операций ограничивается только количеством свободной памяти контроллера;

– Поддержка интерфейса для программирования и отладки: Ethernet, USB, RS-232 (Debug).

Также контроллеры имеют одобрение морским регистром судоходства, что позволяет использовать эти контроллеры для автоматизации судовых систем.

Список литературы

1. Материалы по контроллеру Овен ПЛК110/160. [Электронный ресурс] Режим доступа: http://www.owen.ru .Дата обращения 25.04.2017г.

2. Материалы по CODESYS v.2 - CODESYS 2.3. [Электронный ресурс] Режим доступа: http://www.owen.ru/catalog/codesys_v2/opisanie. Дата обращения 25.04.2017г.

УДК 656.61.052.65.011.56 (0.75.8)

Комаровский Юрий Александрович,
к. т. н., консультант ДВО РАТ
komarovskiy.yu.a@gmail.com

ТОЧНОСТЬ ОПРЕДЕЛЕНИЯ ВОЗВЫШЕНИЙ АНТЕННЫ СУДОВОГО ПРИЁМНИКА GP-37 ВБЛИЗИ СТАНЦИИ DGPS

Отмена в 2000 году режима избирательной доступности (режима S/A – Selective Availability) повлекла увеличение точности определения координат гражданскими приёмниками спутниковой радионавигационной системы (СРНС) Навстар GPS. Кроме того, это подтолкнуло проектантов и изготовителей к выпуску более точных приёмников. Типичным образцом такого прибора служит судовой GPS-приёмник GP-37, изготавливаемый японской компанией Furuno. С его помощью можно определять плановые координаты антенны с точностью на уровне ±1,6 м (с вероятностью 0,68) без приёма дифференциальных поправок. Благодаря этому, приёмник GP-37 нашёл широкое применение не только для решения традиционных задач навигации, но и стал включаться в системы автоматизированных швартовок, в системы динамического позиционирования, в системы автоматического вождения судов, а также в системы мониторинга подводных ланд-

шафтов. В последние годы приёмник GP-37 и его модификации стали использоваться и на суше для сбора, корректировки и пополнения данных географических информационных систем (ГИС), проблемно ориентированных на решение проблем безопасности на транспорте и экологических проблем.

В период времени, когда действовал режим S/A, GPS-приёмники определяли широту и долготу с большей точностью, нежели возвышение фазового центра антенны над геоидом. Ожидалось, что отмена режима S/A в совокупности с дифференциальным режимом работы GPS-приёмников продемонстрирует более высокую точность определения возвышений. Однако анализ результатов экспериментов, проведённых автором с участием различных GPS-приёмников, не позволяет однозначно подтвердить эти ожидания [1-5]. Было высказано предположение о том, что отсутствие заметного увеличения точности возвышения происходило из-за влияния пространственной декорреляции, так как расстояния в экспериментах между DGPS-станцией на мысе Поворотном и испытуемыми GPS-приёмниками во Владивостоке превосходили 56 миль (100 км). Поэтому понадобился эксперимент, в котором GPS-приёмник располагался вблизи дифференциальной станции. Цель данной статьи заключается в обработке и анализе результатов этого эксперимента, чтобы проверить присутствие влияния расстояния до дифференциальной станции на точность определения координат.

Наблюдения за работой судового приёмник GP-37 проводились автором с 9 октября по 20 октября 2012 года. Общая продолжительность записи данных длилась 284 часов 24 минуты, то есть 11,85 суток. В этот период времени число работавших спутников системы Навстар GPS составляло 30 космических аппаратов. Приёмник был установлен на неподвижном основании на берегу бухты Гранитной (Шепалово) между мысом Поворотным и мысом Гранитным непосредственно на берегу Японского моря. Расстояние между антенной дифференциальной станции мыса Поворотного и антенной GP-37 составляло 2,48 мили (4,59 км). Приёмник GP-37 всё время наблюдений находился в автоматическом режиме приёма дифференциальных поправок. При этом он отображал несущую частоту передатчика DGPS 306,5 кГц и темп передачи информации 200 BPS. Мощность принимаемого сигнала колебалась возле величины 55,0 dB, с отношением сигнала к шуму (SNR) 22,0 dB. Мощность передатчика станции DGPS мыса Поворотного заявлена в 400 Ватт.

Данные от приёмника GP-37 в формате NMEA-0183 каждую секунду автоматически записывались на жёсткий диск ноутбука. Всего за время наблюдений было зарегистрировано 937477 измерений возвышения антенны GP-37 над геоидом. Из них 5525 измерений (0,59%) происходили без приёма дифференциальных поправок. Можно предположить, что они про-

сто не транслировались передатчиком станции мыса Поворотного. Эти измерения не обрабатывались.

На первом этапе обработки собранного статистического материала были подсчитаны частоты, с которыми регистрировались те или иные значения возвышения антенны GP-37. По этим данным была построена гистограмма эмпирического распределения возвышений, которую можно видеть на рис. 1.

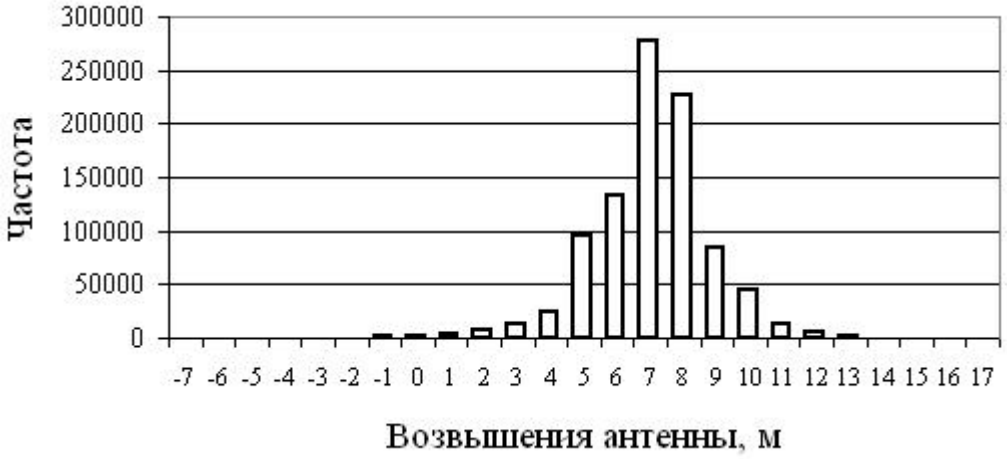

Рис. 1. Гистограмма распределения возвышения антенны

Для получения статистических характеристик распределения возвышений над геоидом антенны приёмника GP-37, работавшего в дифференциальном режиме, возвышение рассматривается в качестве непрерывной случайной величины. Обозначим её через h. Статистические характеристики распределения случайной величины h получим с помощью моментов.

Первый начальный момент случайной величины μ_1 является характеристикой положения и называется математическим ожиданием.

$$\mu_1 = \int_{-\infty}^{\infty} hf(h)dh, \qquad (1)$$

где $f(h)$ – плотность распределения случайной величины, или дифференциальный закон, представляющий собой производную функции распределения. О форме кривой плотности распределения возвышения антенны можно судить по виду гистограммы рис. 1.

Приёмник GP-37 определяет возвышения с разрядностью 1 м. Следовательно, в ходе наблюдений накапливались дискретные случайные величины, принимающие значения h_i . Для них точечной оценкой математического ожидания служит величина M_0, которая рассчитывается по формуле (2).

$$M_0 = \sum_{i=1}^{n} h_i p_i, \qquad (2)$$

где p_i – относительная частота, с которой значение h_i встречалось в наблюдениях; $p_i = n_i/N$, где n_i – частота, с которой регистрировалось значения h_i в данной выборке, N – объём выборки.

Величину M_0 принято называть выборочным средним. С помощью выборочного среднего оценивается математическое ожидание исследуемой совокупность реализуемой случайной величины h. По величине выборочного среднего можно судить о том значении h, возле которого концентрируются измеренные значения возвышения h_i.

В качестве меры рассеивания случайной величины возле математического ожидания в математической статистике принято использовать центральный момент второго порядка μ_2, называемый дисперсией. Для непрерывной случайной величины центральный момент второго порядка записывается в виде следующей формулы:

$$\mu_2 = \int_{-\infty}^{\infty} (h - \mu_1)^2 \, f(h) dh. \qquad (3)$$

В прикладном статистическом анализе, когда исследуемая варианта принимает дискретные значения, точечную оценку дисперсии D вычисляют по формуле (4).

$$D = \sum_{i=1}^{n} (h_i - M_0)^2 \, p_i \, . \qquad (4)$$

Когда исследуется точность каких-либо измерений, то применяют более чувствительную характеристику рассеивания, называемую средним квадратическим отклонением (СКО) и чаще всего обозначаемую буквой σ. Точечная оценка дисперсии и СКО связаны следующим образом: $D = \sigma^2$. Для сравнения между собой случайных компонент измерений приборов, как правило, применяют СКО. Надо заметить, что выборочное среднее и СКО имеют размерность измеряемой величины.

Представление о предельной величине рассеивания случайной величины даёт размах варьирования. Размахом варьирования является абсолютная разность между максимальным значением и минимальным значением измеряемой величины.

Третий центральный момент μ_3 в статистических исследованиях используется для оценки симметричности распределения случайной величины относительно его математического ожидания. Его называют асимметрией, или скошенностью.

$$\mu_3 = \int_{-\infty}^{\infty} (h - \mu_1)^3 \, f(h) dh. \qquad (5)$$

Точечная оценка асимметрии M_3 для случая дискретной случайной величины рассчитывается по формуле (6).

$$M_3 = \sum_{i=1}^{n} (h_i - M_0)^3 \, p_i \, . \qquad (6)$$

Если распределение симметрично, то $\mu_3 = 0$. Тогда при $N \to \infty$, $M_3 \to 0$. Если распределение несимметрично, то M_3 может принимать положительные или отрицательные значения. Неудобство показателя M_3 состоит в том, что он имеет размерность куба случайной величины. Если она мала, то с помощью M_3 становится сложнее сравнивать между собой асимметрии разных величин. Асимметрии становятся во много раз меньше и теряют свойство рельефности, требуемое от показателей. Поэтому в практике оценки точности измерений используется коэффициент асимметрии A, который вычисляется нормированием M_3 кубом СКО,

$$A = \frac{M_3}{\sigma^3} = \frac{\sum_{i=1}^{n} (h_i - M_0)^3 \, p_i}{\sigma^3} \, . \qquad (7)$$

Коэффициент асимметрии A является безразмерной величиной, принимающей положительные и отрицательные значения. Если коэффициент A положителен, то вид плотности распределения имеет левую скошенность. У такого распределения мода (значение h, имеющее наибольшую частоту), всегда меньше M_0. Тогда более вытянутая часть гистограммы будет находиться правее моды. Если коэффициент A отрицателен, то значение моды всегда больше M_0, а вытянутая часть гистограммы будет находиться левее моды. Абсолютная величина коэффициента A указывает на то, насколько асимметрия M_3 больше или меньше M_0. Благодаря этому свойству, с помощью коэффициента A можно сравнивать между собой скошенности распределений разных случайных величин. Если коэффициент A в разных выборках одной и той же случайной величины устойчиво положителен или устойчиво отрицателен, то по этому признаку нельзя рассматривать распределение такой случайной величины подчинённое закону Гаусса.

Четвёртый центральный момент μ_4 служит для оценки так называемой островершинности распределения случайной величины.

$$\mu_4 = \int_{-\infty}^{\infty} (h - \mu_1)^4 \, f(h) dh. \qquad (8)$$

Точечная оценка четвёртого центрального момента M_4 вычисляется по формуле (9).

$$M_4 = \sum_{i=1}^{n} (h_i - M_0)^4 \, p_i \, . \qquad (9)$$

У закона распределения Гаусса есть свойство: $\mu_4 / (\mu_2)^2 = 3$. Следовательно, если измеряемая случайная величина распределена по закону Гаусса, то при $N \to \infty$ $(M_4 / \sigma^4) \to 3$. На этом свойстве основан показатель островершинности, называемый эксцессом E. $E = [M_4 / \sigma^4]-3$. Если эксцесс близок к 0, то распределение случайной величины близко к распределению Гаусса. Когда эксцесс положителен, то гистограммы в области среднего выборочного будут располагаться выше кривой плотности распределения Гаусса. При отрицательном эксцессе у гистограммы будет плоская вершина, а график кривой Гаусса в области среднего выборочного будет выше частот. Таким образом, величина выборочного эксцесса при больших выборках может использоваться для проверки выполнимости закона Гаусса.

По приведённым выше формулам, а также с помощью методов, разработанных автором для вычисления моды и медианы [6], были рассчитаны характеристики распределения измеренных возвышений антенны приёмника GP-37, работавшего в дифференциальном режиме вблизи DGPS-станции мыса Поворотного с 9 по 20 октября июля 2012 года. Результаты вычислений представлены в табл. 1.

Таблица 1

Статистические характеристики распределения измеренных возвышений антенны приёмника GP-37, работавшего в дифференциальном режиме в октябре 2012 года в Шепалово

Статистическая характеристика	Величина
Выборочное среднее, м	7,1145
Среднее квадратическое отклонение, м	1,7446
Мода, м	7,3625
Медиана, м	6,6603
Асимметрия	– 0,4312
Эксцесс	2,6371
Максимальное значение, м	17
Минимальное значение, м	– 7
Размах варьирования, м	24
Объём выборки	931952

Наиболее показательной характеристикой точности в табл. 1 является СКО. Среднее квадратическое отклонение возвышения антенны в эксперименте в Шепалово составило 1,7446 м. Здесь полезно сравнить этот ре-

зультат с результатами, полученными в экспериментальных наблюдениях за работой GPS-приёмников в дифференциальном режиме.

В декабре 2007 года автором начались наблюдения за работой приёмника J-NAV500, установленного в лаборатории кафедры технических средств судовождения МГУ им. адм. Г. И. Невельского. Наблюдения продолжались до 4 июля 2008 года. Обработка этого материала позволила оценить СКО возвышения как 2,206 м [2]. В 2010 году (с 10 по 18 июля) автор провёл экспериментальные наблюдения с участием приёмника GP-37 в Уссурийской астрофизической обсерватории ДВО РАН. Там СКО возвышения антенны оценивалось в 2,1699 м. С 11 июня по 4 августа 2011 года подобные наблюдения за работой приёмника GP-37 выполнялись автором во Владивостоке в районе горы Буссе. Тогда СКО возвышения составило 2,7179 м [5]. Сравнение этих результатов позволяет сделать предварительный вывод об увеличении точности определения возвышений антенны GPS-приёмника по мере приближения к дифференциальной станции.

Следует отметить также небольшой размах варьирования возвышений в табл. 1. Как и в предыдущих экспериментальных исследованиях, результаты обработки данных Шепалово демонстрируют отрицательную асимметрию и высокое значение положительной островершинности. Сочетание полученных асимметрии и эксцесса не позволяет предполагать подчинение распределения возвышений закону Гаусса. Обнаружение значительного снижения (почти на 35%) влияния случайных погрешностей определения возвышений антенны GPS-приёмника, установленного рядом с дифференциальной станцией, нельзя пока признать полностью достоверным фактом. Необходимы повторения подобных экспериментальных работ.

Собранный экспериментальный материал и результаты его обработки позволят расширить область применения судовых GPS-приёмников и послужат базой для дальнейших работ по созданию метода ортометрических высот, повышающего точность определения широт и долгот.

Список литературы

1. Комаровский Ю. А. Особенности применения технологии дифференциальной GPS для изучения высотной поясности объектов экосистем прибрежных территорий // Ю. А. Комаровский. – Вестник Морского государственного университета. Серия: Теория и практика защиты моря. Вып. 34/2009. – Владивосток : Мор. гос. ун-т, 2009. – С. 48-54.

2. Комаровский Ю. А. Определение геодезических высот объектов ГИС GPS-приёмником J-NAV500 в дифференциальном режиме // Ю. А. Комаровский. – Вестник Морского государственного университета. Вып. 28/2008. Серия: Теория и практика защиты моря. Владивосток: Мор. гос. ун-т, 2008. – С. 73-76.

3. Комаровский Ю. А. Сравнительный анализ характеристик точности работы в дифференциальном режиме GPS-приёмника J-NAV500 / Ю. А Комаровский. – Проблемы транспорта Дальнего Востока. Материалы восьмой межд. научн.-практ. конф. 30 сентября – 2 октября 2009 г. – Владивосток: ДВО Российской Академии транспорта, 2009. – С. 79-82.

4. Комаровский Ю. А. Характеристики точности автономного режима работы GPS-приёмника J-NAV500 // Вестник Морского государственного университета. Вып. 32/2009. Серия : Судовождение. – Владивосток : Мор. гос. ун-т, 2009. – С. 60-64.

5. Комаровский Ю. А. Точность дифференциального режима работы приёмника GP-37 при изучении высотного распределения объектов экосистем // Вестник Морского государственного университета. Серия : Теория и практика защиты моря. – Вып. 48/2011. – Владивосток : Мор. гос. ун-т, 2011. – С. 47-53.

6. Комаровский Ю. А. Вычисление непараметрических позиционных характеристик эмпирического распределения погрешностей координат GPS-приёмника // Вестник Морского государственного университета. им. адм. Г.И. Невельского. Серия : Автоматическое управление, математическое моделирование и информационные технологии. Вып. 51/2012. – Владивосток : Мор. гос. ун-т, 2012. – С. 54-60.

УДК 355: 528.2; 623.64

Комаровский Юрий Александрович,
к. т. н., консультант ДВО РАТ
komarovskiy.yu.a@gmail.com

АЛГОРИТМ ПЕРЕХОДА К КООРДИНАТАМ ГЕОДЕЗИЧЕСКОЙ СИСТЕМЫ ГСК-2011

С 1 января 2017 года в Российской Федерации введена в действие новая геодезическая система координат (ГСК-2011), разработанная и принятая в 2011 году. В связи с этим перед отечественными геодезистами и картографами встаёт задача пересчёта координат геодезических пунктов и издания новых карт. У изготовителей приёмников спутниковых радионавигационных систем (СРНС) и устройств отображения электронных карт возникает необходимость выпуска новой навигационной аппаратуры, способной представлять координаты в новой системе ГСК-2011. В мировой практике судовождения принята геодезическая система координат WGS-84 (World Geodetic System 1984 года). Давно морские навигационные карты за рубежом издаются в этой геодезической системе. На отечественных морских картах обязательно указываются поправки для перехода от координат, полученных СРНС-приёмником (от координат в системе WGS-84), к координатам системы данной карты. Следовательно, для работ на новых картах отечественного издания в системе ГСК-2011 потребуются способы перехода от координат WGS-84. В настоящее время пока отсутствуют

формулы для непосредственного перехода от координат системы WGS-84 к координатам системы ГСК-2011. Цель данной статьи заключается в обосновании и представлении одного из возможных способов такого перехода.

Постановлением Совета Министров СССР № 760 от 7 апреля 1946 года “О введении единой системы геодезических координат и высот на территории СССР” учреждалась “Система координат 1942 года”. Постановлением устанавливалось начало координат в Пулково, за исходный уровень абсолютных высот брался нуль Кронштадского футштока, назначался новый референц-эллипсоид с большей полуосью 6378245 м и знаменателем сжатия 299,3. В дальнейшем земной сфероид с такими размерениями стали называть референц-эллипсоидом Красовского 1940 года [1]. Систему координат 1942 года называли ещё Пулково-42 или СК-42. В зарубежной литературе эту систему обозначают как Pulkovo 42, S-42 или SK-42. На отечественных навигационных картах, изданных до 1992 года, эта система указывалась как “Система координат советских морских карт”. Распространение системы координат 1942 года на территорию бывшего СССР проводилось последовательно по блокам: блок Север (1968), блок Крайний Север (1971), блок Дальний Восток (1972) и так далее. Надо отметить, что территория Сахалина, Камчатки и Приморья были привязаны гораздо позже [2]. Способ блочного распространения имел ряд недостатков, но был оправдан тем, что необходимо было в кратчайшие сроки распространить систему координат на всё огромное пространство, обеспечив тем самым возможность сплошного его картографирования. Особо в этом нуждались мореплаватели, так как уже начиналась эра спутниковой навигации, а морские карты, составленные на отечественные воды Дальнего Востока и Севера, не отличались точностью привязки.

По первоначальным планам в соответствии с поручением Правительства СССР 1948 года общее согласование координат должно быть завершено в 1985 году. На самом деле оно было выполнено только в 1991 году, когда СК-42 с позиций спутниковой навигации безнадёжно устарела, так как не была геоцентрической. К тому времени за рубежом в спутниковой навигации использовались системы координат WGS-72 и пришедшая ей на смену WGS-84. Отсутствие высокой точности привязки приводило к большим погрешностям, когда координаты, полученные с помощью судовых приёмников системы Навстар GPS, наносились на отечественные навигационные карты Дальневосточных морей. Практика применения современных спутниковых технологий показала, что эффективное использование спутниковых приёмников навигационных систем Глонасс и Навстар GPS на картах в системе координат 1942 года во многих случаях невозможно. Система координат 1942 года не обеспечивает на требуемом уровне точности однозначного перехода к геоцентрическим системам координат, в которых работают глобальные навигационные системы Глонасс и Навстар GPS. Поэтому постановлением Правительства Российской Фе-

дерации от 28 июля 2000 года № 568 “Об установлении единых государственных систем координат” была введена новая единая государственная система геодезических координат 1995 года (СК-95) для использования в геодезических и картографических работах, начиная с 1 июля 2002 года.

Система координат СК-95 была установлена с условием параллельности осей её референц-эллипсоида пространственным осям геоцентрической системы координат ПЗ-90 (Параметры Земли 1990 года), которая была разработана для обеспечения орбитальных полётов спутников СРНС Глонасс. За отсчётную поверхность в СК-95 был принят тот же референц-эллипсоид Красовского.

Ограничения, обусловленные высоким уровнем внутренних деформаций системы координат 1942 года и, прежде всего, значительной нерегулярностью деформаций, потребовали бы новых обширных геодезических съёмок и переиздания большого количества карт. Средств на эти работы у государства не было. Кроме того, система СК-95 была морально устаревшей ещё до её принятия, так как не являлась геоцентрической. Поэтому до сих пор продолжают сохраняться неудобства, связанные с несоответствием координат отечественных морских карт координатам спутниковых навигационных систем.

Выходом из сложившейся ситуации такой геодезической отсталости могло бы принятие одной из известных международных геодезических систем координат WGS-84 или ITRF (International Terrestrial Reference Frame). Но в нашей стране пошли ставшим уже традиционным путём и решили ввести очередную систему, отличную от международных. Постановлением Правительства РФ от 28 декабря 2012 года № 1463 в качестве новых государственных систем координат с 1 января 2017 года устанавливаются геодезическая система координат 2011 года для геодезических и картографических работ и общеземная геоцентрическая система координат «Параметры Земли 1990 года» (версия ПЗ-90.11) для обеспечения орбитальных полётов и решения навигационных задач [3].

Новая отечественная система ГСК-2011 представляет собой геоцентрическую экваториальную пространственную прямоугольную систему координат. В ней положение потребителя определяется относительно центра масс Земли. Отсчётной плоскостью здесь служит плоскость экватора, проходящей через центр масс Земли. Плоскость нулевого меридиана перпендикулярна ей и проходит через ось вращения Земли. Третья отсчётная плоскость также проходит через ось вращения (через ось Z) и отстоит от плоскости нулевого меридиана на 90° к востоку. Положительное направление оси Z совпадает с направлением вектора угловой скорости Земли. Положительное направление оси X задано от центра Земли по линии пересечения плоскости экватора и плоскости нулевого меридиана. Ось Y принадлежит плоскости экватора, направлена от центра масс Земли и отстоит

от оси X на 90° к востоку. Постановление Правительства назначило параметры нового референц-эллипсоида ГСК-2011. Они приведены в табл. 1 для сравнения с параметрами референц-эллипсоида WGS-84.

Таблица 1

Параметры референц-эллипсоидов ГСК-2011 и WGS-84

Эллипсоид	Большая полуось, м	Знаменатель сжатия	e^2
ГСК-2011	6378136,5	298,2564151	0,00669439809
WGS-84	6378137	298,257223563	0,00669437999

Как следует из табл. 1, параметры этих эллипсоидов почти совпадают. Поэтому в первом приближении координаты, полученные с помощью отечественных приёмников спутниковых навигационных систем Навстар GPS и Глонасс, можно будет напрямую без преобразования наносить на морскую путевую карту в системе WGS-84. Как показывают расчёты, линейные параметры преобразования ГСК-2011 по отношению к International Terrain Reference Frame 2008 года (ITRF-2008) составляют менее 3 см, а углы Эйлера и масштабный коэффициент равны нулю. Если учесть, что Европа и Китайская Народная Республика в своих спутниковых навигационных системах используют ITRF-2008, то переход России к системы ГСК-2011 приведёт к возникновению единого непрерывного Евразийского геодезического пространства.

С появлением судовых спутниковых приёмников, способных определять точные текущие координаты в системе ГСК-2011, потребует контроля над точностью перехода от координат в системе WGS-84. Решение этой задачи станет более востребованным после поступления на отечественные суда так называемых мультисистемных СРНС-приёмников, способных одновременно принимать сигналы спутников Навстар GPS, Глонасс, Галилео и Бейдоу. Для решения задачи можно воспользоваться высокоточным методом Гельмерта и параметрами перехода, вычисленными для ПЗ-90.11 следующим образом: сначала осуществляется переход от координат в WGS-84 к координатам в ПЗ-90.11, а затем – от координат в ПЗ-90.11 к искомым координатам в ГСК-2011. Высокоточные параметры таких переходов уже опубликованы в [4].

Рассмотрим точный способ Гельмерта для перехода от прямоугольных пространственных координат системы A (X_A, Y_A, Z_A) к прямоугольным пространственным координатам системы B. Для этого воспользуемся алгоритмом, изложенным в работе [2]. В матричной форме способ Гельмерта имеет следующий вид:

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix}_B = (1+\Delta m)\times R \times \begin{bmatrix} X \\ Y \\ Z \end{bmatrix}_A + \begin{bmatrix} \Delta X \\ \Delta Y \\ \Delta Z \end{bmatrix},$$

где ΔX, ΔY, ΔZ – элементы линейного взаимного ориентирования, то есть отстояния центров референц-эллипсоидов; Δm – масштабный множитель, учитывающий разницу в расстояниях на поверхностях эллипсоидов; R – матрица вращения;

$$R = R_X \times R_Y \times R_Z,$$

где R_X, R_Y, R_Z – матрицы вращения вокруг осей X, Y, Z, соответственно;

$$R_Z = \begin{bmatrix} \cos\varepsilon_Z & \sin\varepsilon_Z & 0 \\ -\sin\varepsilon_Z & \cos\varepsilon_Z & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad R_Y = \begin{bmatrix} \cos\varepsilon_Y & 0 & -\sin\varepsilon_Y \\ 0 & 1 & 0 \\ \sin\varepsilon_Y & 0 & \cos\varepsilon_Y \end{bmatrix},$$

$$R_X = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\varepsilon_X & \sin\varepsilon_X \\ 0 & -\sin\varepsilon_X & \cos\varepsilon_X \end{bmatrix},$$

где ε_X, ε_Y, ε_Z – углы вращения вокруг осей X, Y, Z, соответственно.

Угол вращения считается положительным, когда вращение усматривается по часовой стрелке, если смотреть по соответствующей оси из начала координат в сторону положительного направления оси. Углы вращения в расчётах участвуют в радианах или в секундах.

После перемножения матрица вращения R примет такой вид:

$$R = \begin{bmatrix} r_{11} & r_{12} & r_{13} \\ r_{21} & r_{22} & r_{23} \\ r_{31} & r_{32} & r_{33} \end{bmatrix}, \qquad (1)$$

где $r_{11} = \cos\varepsilon_Z \cos\varepsilon_Y$, $r_{12} = \cos\varepsilon_Z \sin\varepsilon_Y \sin\varepsilon_X + \sin\varepsilon_Z \cos\varepsilon_X$,

$r_{13} = \sin\varepsilon_Z \sin\varepsilon_X - \cos\varepsilon_Z \sin\varepsilon_Y \cos\varepsilon_X$, $r_{21} = -\sin\varepsilon_Z \cos\varepsilon_Y$,

$r_{22} = \cos\varepsilon_Z \cos\varepsilon_X - \sin\varepsilon_Z \sin\varepsilon_Y \sin\varepsilon_X$,

$r_{23} = \sin\varepsilon_Z \sin\varepsilon_Y \cos\varepsilon_X + \cos\varepsilon_Z \sin\varepsilon_X$,

$r_{31} = \sin\varepsilon_Y$, $r_{32} = -\cos\varepsilon_Y \sin\varepsilon_X$, $r_{33} = \cos\varepsilon_Y \cos\varepsilon_X$.

Поскольку углы вращения, как правило, малы, то для большинства приближённых расчётов элементы матрицы (1) заменяют на углы. Тогда матрица вращения становится такой:

$$R \approx \begin{bmatrix} 1 & \varepsilon_Z & -\varepsilon_Y \\ -\varepsilon_Z & 1 & \varepsilon_X \\ \varepsilon_Y & -\varepsilon_X & 1 \end{bmatrix}. \qquad (2)$$

Для приближённых расчётов используют матрицу вращения (2) и допускают, что масштабный множитель $\Delta m = 0$. Тогда вычисления прямоугольных пространственных координат в геодезической системе B проводятся по упрощенным формулам (3):

$$\left.\begin{aligned} X_B &= X_A + Y_A\varepsilon_Z - Z_A\varepsilon_Y + \Delta X \\ Y_B &= Y_A + Z_A\varepsilon_X - X_A\varepsilon_Z + \Delta Y \\ Z_B &= Z_A + X_A\varepsilon_Y - Y_A\varepsilon_X + \Delta Z \end{aligned}\right\}. \qquad (3)$$

Формула для расчёта прямоугольных пространственных координат для перехода от WGS-84 версии G1150, принятой 20 января 2002 года, к ПЗ-90.11 имеет следующий вид [4]:

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix}_{\text{ПЗ}} = (1 - 0{,}008\times10^{-6}) \begin{bmatrix} 1 & -2{,}04107\times10^{-8} & -1{,}71624\times10^{-8} \\ +2{,}04107\times10^{-8} & 1 & -1{,}11507\times10^{-8} \\ +1{,}71624\times10^{-8} & -1{,}11507\times10^{-8} & 1 \end{bmatrix} \begin{bmatrix} X \\ Y \\ Z \end{bmatrix}_{\text{WGS}} - \begin{bmatrix} -0{,}003 \\ -0{,}001 \\ 0 \end{bmatrix},$$

где углы Эйлера даны в радианах.

В угловых секундах они имеют следующие значения:

$$\varepsilon_X = -0{,}0023'', \quad \varepsilon_Y = +0{,}00354'', \quad \varepsilon_Z = -0{,}00421''.$$

Далее производится переход от координат в системе ПЗ-90.11 к координатам в системе ГКС-2011 с помощью аналогичной формулы и параметров [4].

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix}_{\text{ГСК}} = (1 + 0{,}006\times10^{-6}) \begin{bmatrix} 1 & -2{,}56951\times10^{-10} & -9{,}21146\times10^{-11} \\ +2{,}56951\times10^{-10} & 1 & +2{,}72465\times10^{-9} \\ +9{,}21146\times10^{-11} & -2{,}72465\times10^{-9} & 1 \end{bmatrix} \begin{bmatrix} X \\ Y \\ Z \end{bmatrix}_{\text{ПЗ}} - \begin{bmatrix} 0 \\ +0{,}014 \\ -0{,}008 \end{bmatrix},$$

Углы Эйлера, выраженные в угловых секундах, для данного преобразования координат имеют следующие значения:

$$\varepsilon_X = +0{,}000562'', \quad \varepsilon_Y = +0{,}000019'', \quad \varepsilon_Z = -0{,}000053''.$$

Анализ точности преобразования прямоугольных координат приближённым способом (с помощью матрицы вращения (2) и при нулевом значении масштабного множителя), выполненный в работе [2], показал, что точность будет на уровне ±0,3 м. Такая точность вполне приемлема для решения большинства задач высокоточного судовождения.

В геодезии и в судовождении используются геодезические координаты. К ним относятся широта (φ), долгота (λ) и возвышение над поверхностью референц-эллипсоида (*h)*. Широты и долготы являются угловыми величинами, а возвышение принято измерять в метрах. Чтобы исходные координаты (φ, λ, *h*) преобразовать в пространственные прямоугольные (*X*, *Y*, *Z*), которые измеряются в метрах, следует воспользоваться следующими формулами:

$$\begin{cases} X = (N + h)\cos\varphi\cos\lambda, \\ Y = (N + h)\cos\varphi\sin\lambda, \\ Z = \left[(1 - e^2)N + h\right]\sin\varphi, \end{cases}$$

где *N* – радиус кривизны в первом вертикале референц-эллипсоида WGS-84,

$$N = \frac{a}{\sqrt{1 - e^2 \sin^2 \varphi}},$$

где a – большая ось референц-эллипсоида WGS-84, e^2 – квадрат первого эксцентриситета референц-эллипсоида WGS-84.

Величины a и e^2 содержатся в табл. 1.

После вычисления прямоугольных пространственных координат в новой системе ГКС-2011 необходимо их преобразовать в геодезические координаты. В настоящее время разработаны прямые и итерационные способы расчётов геодезических координат. Рассмотрим итерационный способ, изложенный в ГОСТ 32453 [4].

На первом этапе вычислений получают вспомогательную величину D.

$$D = \sqrt{X^2 + Y^2}\ .$$

Если $D = 0$, то искомые широта в радианах и возвышение в метрах определятся из формул

$$\varphi = \frac{\pi}{2} \cdot \frac{Z}{|Z|}, \quad \lambda = 0\,, \quad h = Z \sin\varphi - a\sqrt{1 - e^2 \sin^2 \varphi}\ .$$

Здесь a и e^2 уже являются параметрами референц-эллипсоида ГСК-2011. Они помещены в табл. 1.

Если $D \neq 0$, то искомая долгота λ в радианах вычисляется по следующим правилам:

$$\lambda_A = \left| \arcsin\left(\frac{Y}{D}\right) \right|;$$

если $Y < 0, X > 0$, то $\lambda = 2\pi - \lambda_A$; если $Y < 0, X < 0$, то $\lambda = \pi + \lambda_A$;
если $Y > 0, X < 0$, то $\lambda = \pi - \lambda_A$; если $Y > 0, X > 0$, то $\lambda = \lambda_A$;
если $Y = 0, X > 0$, то $\lambda = 0$; если $Y = 0, X < 0$, то $\lambda = \pi$.

Если $Z = 0$, то $\varphi = 0$, $h = D - a$. Если $Z \neq 0$, то вычисляются вспомогательные величины r, c, p,

$$r = \sqrt{X^2 + Y^2 + Z^2}\ , \quad c = \arcsin\left(\frac{Z}{r}\right), \quad p = \frac{e^2 a}{2r},$$

и запускается процесс итераций, используя величины s_1 и s_2.

На первом шаге s_1 получает нулевое значение. Затем вычисляются b, s_2 и d,

$$b = c + s_1\ , \tag{4}$$

$$s_2 = \arcsin\left(\frac{p \sin(2b)}{\sqrt{1 - e^2 \sin^2 b}}\right), \quad d = \left|s_2 - s_1\right|.$$

Если значение d меньше наперёд заданного допуска, определяющего точность вычислений, то

$$\varphi = b\,, \quad h = D\cos\varphi + Z\sin\varphi - a\sqrt{1 - e^2\sin^2\varphi}\,.$$

Если d равно или больше наперёд заданного допуска, то $s_1 = s_2$, и вычисления повторяют, начиная с формулы (4).

Предлагаемый алгоритм перехода от координат системы WGS-84 к координатам системы ГСК-2011 прост, но его реализация требует высокой разрядности вычислений.

Список литературы

1. Телеганов Н. А., Тетерин Г. Н. Метод и системы координат в геодезии. Учеб. пособие. – Новосибирск: ГОУ ВПО «Сибирская государственная геодезическая академия», 2008. 143 с.

2. Комаровский Ю. А. Использование различных референц-эллипсоидов в судовождении: Учеб. пособие. Изд. второе, перераб. и дополн. – Владивосток: Мор. гос. ун-т, 2005. 341 с.

3. Правительство Российской Федерации. Постановление от 28 декабря 2012 года № 1463 «О единых государственных системах координат».

4. ГОСТ 32453. Межгосударственный стандарт. Глобальная навигационная спутниковая система. Система координат. Методы преобразования координат определяемых точек. – М.: Стандартинформ, 2016. 42 с.

УДК 656.62.052.4

Комаровский Юрий Александрович,
к. т. н., консультант НИИ ДВО РАТ
komarovskiy.yu.a@gmail.com

СВОЙСТВА ГОРИЗОНТАЛЬНОГО ГЕОМЕТРИЧЕСКОГО ФАКТОРА СУДОВОГО GPS/GLONASS-ПРИЁМНИКА SGN-500

Одной из проблем, которая сопутствует эксплуатацию современных судовых приёмников спутниковых радионавигационных систем (СРНС), является проблема оперативной оценки получаемых в данный момент времени координат. В доспутниковой навигации были разработаны многочисленные визуальные и радиотехнические способы определения места судна и методы оценки их точности. Штурман, исходя из навигационной обстановки, старался применять такой способ, который в данный момент времени обеспечивал быстрое и наиболее точное получение координат судна. Появление на судах СРНС-приёмников, с одной стороны, освободило штурмана от выполнения измерений навигационных параметров, их обработки, вычисления координат и выполнения графических построений на карте. С другой стороны, штурман перестал быть участником технологического процесса получения координат судна. А точность предоставляемых ему координат изготовители спутниковой навигационной аппаратуры

предлагают оценивать с помощью косвенного показателя, который в отечественной литературе принято называть горизонтальным геометрическим фактором (ГГФ). В англоязычной литературе он обозначается как HDOP (Horizontal Dilution of Precision). Считается, что чем меньше величина ГГФ, отображаемая в данный момент на дисплее СРНС-приёмника, тем точнее текущие координаты.

В существующей литературе по СРНС погрешность определения места потребителя принято выражать в виде следующего произведения:

$$\sigma = HDOP \times \sigma_P ,$$

где σ – радиальная средняя квадратическая погрешность места судна, σ_P – средняя квадратическая погрешность измерений псевдорасстояний до всех спутников, принятых для данной обсервации,

$$\sigma_P = \sqrt{\frac{\sum_{i=1}^{n} \sigma_{S_i}^2}{n}} ,$$

где σ_{Si} – средняя квадратическая погрешность измерения псевдорасстояния до *i*-го спутника из числя принятых для данной обсервации, *n* – число спутников, принятых для данной обсервации.

Величина HDOP зависит от геометрии взаимного расположения радиовидимых спутников и антенны судового приёмника. Горизонтальный геометрический фактор (HDOP), как выяснилось, может вычисляться в каждом типе СРНС-приёмника по-разному [1,2]. На первых этапах развития СРНС Навстар GPS из-за ограниченного числа спутников в видимом над горизонтом созвездии геометрия их расположения играла существенную роль. Поэтому в том классическом представлении HDOP, в котором этот показатель рассчитывается по четырём спутникам рабочего созвездия, он был достаточно чувствительным [3]. Более того, компонента геометрии расположения спутников в показателе HDOP превосходила компоненту случайной погрешности измерения псевдодальностей. А поскольку до недавнего времени действовал режим избирательной доступности, который искусственно понижал точность определения псевдодальностей как минимум на порядок, то эта компонента существенной роли не играла. В настоящее время число действующих спутников СРНС Навстар GPS иногда доходит до 32, причём, над горизонтом порой можно одновременно наблюдать более 12 спутников. В такой ситуации те приёмники системы Навстар GPS, которые рассчитывают HDOP по четырём спутникам, как это до сих пор рекомендует документ [3], делает этот показатель весьма малочувствительным. Происходит это из-за того, что при большом числе спутников над горизонтом приёмник все-

гда в состоянии подобрать такое рабочее созвездие из четырёх, которое даст в итоге наименьшее HDOP. В литературе последних лет уже предлагается их делить на геометрические HDOP и математические HDOP [2]. Геометрическими HDOP считаются те, которые рассчитаны по четырём спутникам рабочего созвездия, а математическими HDOP – по всем спутникам, сигналы которых используются для определения места судна. В экспериментальных наблюдениях, выполненных автором, математические HDOP показали более высокую чувствительность по сравнению с геометрическими HDOP.

Другой недостаток существующих алгоритмов расчёта горизонтального геометрического фактора заключается в произволе назначения величины дисперсии погрешности измерения псевдодальностей. В существующей литературе отсутствуют рекомендации по их заданию. Поэтому каждый изготовитель навигационных приёмников и разработчик программного обеспечения к ним волен назначать их по собственному усмотрению. Следовательно, по причине не установленных правил задания случайной компоненты горизонтального геометрического фактора возникает неоднозначность в показаниях величин HDOP разных приёмников, одновременно работающих в одинаковых условиях.

В последние три года на отечественные суда стали поступать мультисистемные СРНС-приёмники, способные одновременно принимать сигналы спутников двух и более навигационных спутниковых систем. Примером такого прибора является двухсистемный GPS/Glonass-приёмник SGN-500, который изготавливается компанией Samyung (Республика Корея). Поскольку опыт эксплуатации двухсистемных судовых СРНС-приёмников отсутствует, то возникает потребность рассмотреть свойства вычисляемых ГГФ и сравнить их величины с величинами ГГФ параллельно работающих других приёмников. Так как таких сведений не обнаружено, то было принято решение провести экспериментальные наблюдения за работой приёмника SGN-500 и GP-37. Наблюдения проводились на патрульном судне Дальневосточного управления государственного морского надзора летом и осенью 2016 года. На нём приёмник SGN-500 входил в состав навигационного комплекса. Приёмник GP-37 устанавливался на время проведения синхронных наблюдений. Антенны приёмников располагались на одном уровне и на расстоянии 0,92 м друг от друга.

В результате обработки синхронно зарегистрированных данных оказалось, что всегда значения ГГФ SGN-500 почти в два раза превосходили соответствующие им значения ГГФ GP-37. Характер изменения значений ГГФ SGN-500 существенно отличается от характера изменения значений ГГФ GP-37. Иллюстрацией тому могут послужить графики рис. 1, полученные по результатам 2-х часовых наблюдений 23 сентября

2016 года на ошвартованном судне в гавани яхт-клуба Морского государственного университета (МГУ) им. адм. Г.И. Невельского во Владивостоке [4].

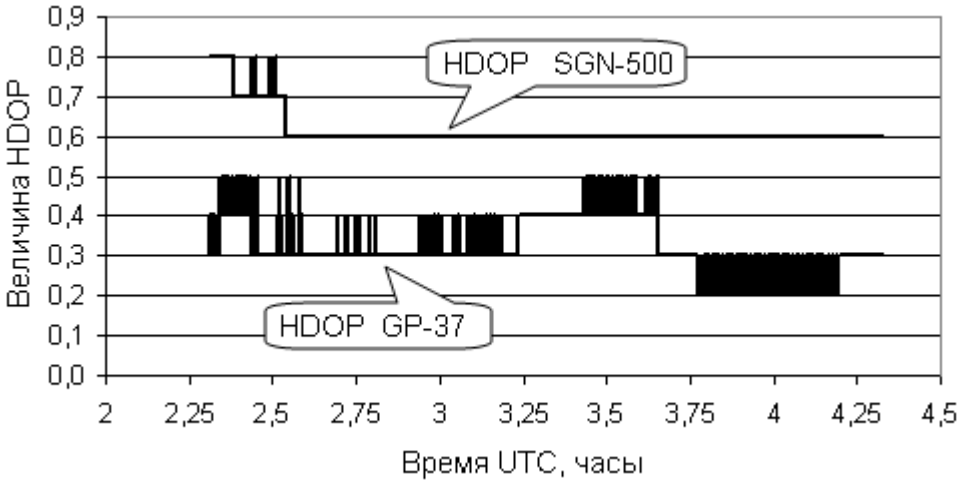

Рис. 1. Изменение HDOP SGN-500 и GP-37 26 сентября 2016 года

Полученный результат располагает к продолжению экспериментов для выяснения того, как точно приёмник SGN-500 определяет обсервованные координаты и вычисляет ГГФ, принимая сигналы спутников либо СРНС Глонасс, либо Навстар GPS. К сожалению, изучаемый приёмник не имеет возможности задания работы от конкретной спутниковой навигационной системы.

Величина HDOP, вычисляемая приёмником в данный момент, зависит от геометрии расположения спутников относительно судовой антенны. А так как движение спутников строго предсказуемо, то характер изменения HDOP для одного и того же места на поверхности Земли будет сдвигаться во времени от суток к суткам в среднем на 4 минуты. Иными словами, характерные точки графика изменения HDOP в следующих сутках будут наступать на 4 минуты раньше. Это явление хорошо просматривается в графиках HDOP GP-37, обнаруженное автором ранее. Приёмник SGN-500 работает по сигналам сразу двух СРНС. Поэтому возникает желание проверить проявление этой закономерности в двухсистемном приёмнике. С этой целью были произведены 2-х часовые регистрации HDOP приёмника SGN-500 в течение ряда суток. Регистрации начинались ровно в 10 часов Владивостокского времени (в 0 часов UTC). На судне отсутствовала возможность автоматической регистрации на жёсткий диск ноутбука генерируемой приёмником SGN-500 информации. Поэтому данные, выводимые на экран дисплея приёмника, пришлось фиксировать с помощью цифровой видеокамеры с последующим переформатированием вручную в файлы Excel. Результаты обработки данных, записанных 21, 25, 28 и 29 июля, представлены на рис. 1.

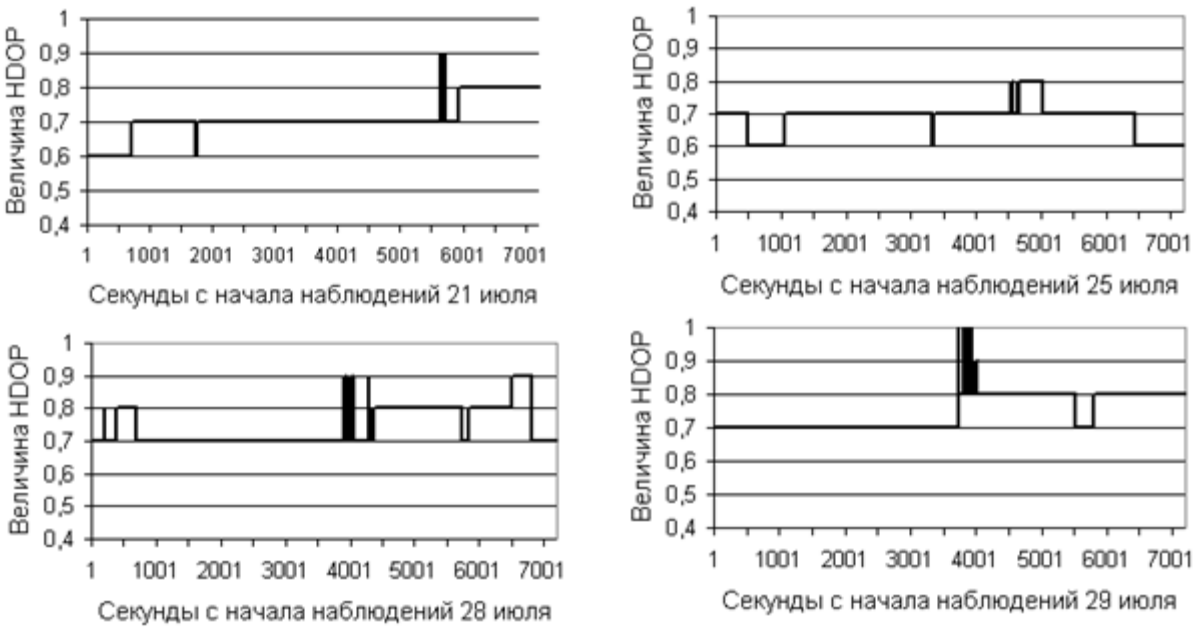

Рис. 2. Наблюдения HDOP SGN-500 в июле 2016 года

Анализ графиков рис. 1 позволяет сделать следующие выводы. В наблюдениях 21 и 25 июля наблюдаются всплески величин HDOP, происходящие между 5000-м и 6000-м наблюдениями. Начало импульса 21 июля произошло на 5657-й секунде наблюдений, а 25-го импульс начался на 4558-й секунде, то есть на 18,3 минуты раньше. Это ненамного больше ожидаемых 16 минут. Приблизительно такой же импульс наблюдается на графиках 28 и 29 июля. Их передние фронты наступали на 3905-й секунде и на 3818-й секунде соответственно. Разница составила всего 1,45 минуты вместо ожидаемых 4 минут. Такие результаты на позволяют с уверенностью говорить о присутствии ожидаемой закономерности в характере изменения HDOP приёмника SGN-500.

С целью разрешения данной неопределённости были предприняты дополнительные 2-х часовые наблюдения 1, 2, 3 и 9 августа, также начинавшиеся в 10 часов. Графики изменения ГГФ в эти дни можно видеть на рис. 3.

На графиках рис. 3 также можно наблюдать характерный всплеск значения HDOP от величины 0,7. За сутки с 1-го августа он сместился по оси времени на 5 минут, со 2-го августа он сместился на 4,1 минуту. За 6 суток с 3-го по 9 августа он стал наступать на 32 минуты раньше. Поэтому что касается повторяемости значений ГГФ, вычисляемых приёмником SGN-500, если предположить её существование, то она, возможно, проявляется только на периоде времени не более одних суток. Поэтому трудно будет прогнозировать в работе приёмника SGN-500 наступление моментов

времени, когда обсервации возможны с большей или с меньшей точностью.

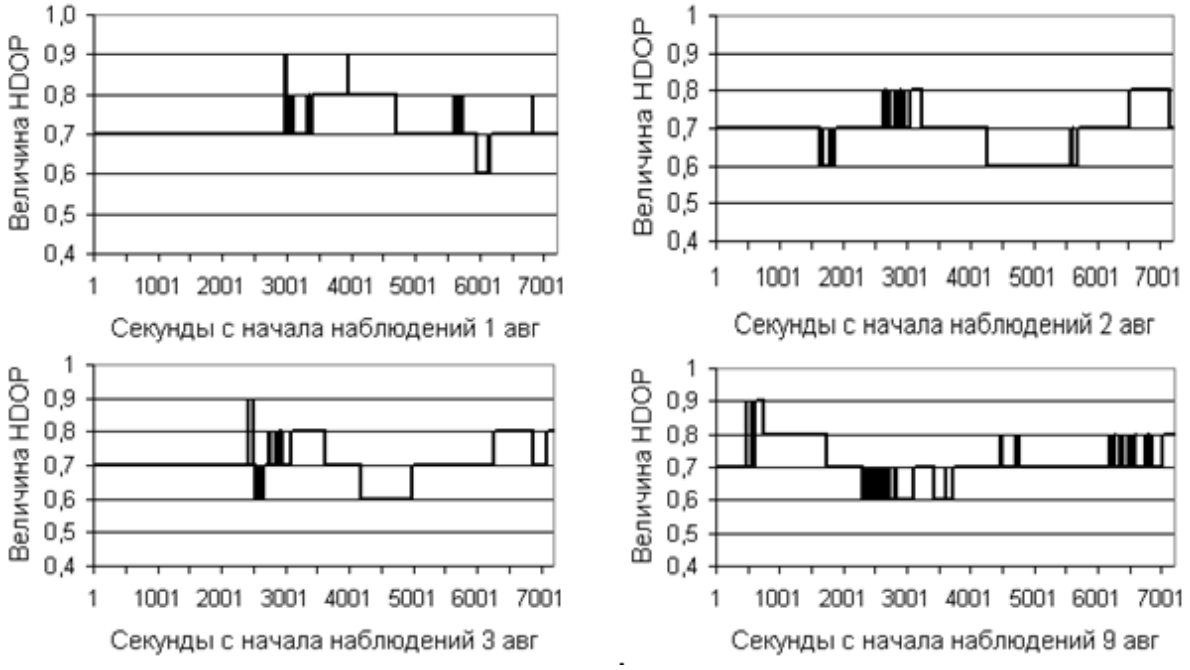

Рис. 3. Наблюдения HDOP SGN-500 в августе 2016 года

Несомненный интерес представляют параметры распределения величин HDOP приёмника SGN-500. Для получения этих данных были проанализированы результаты обработки всех наблюдений за работой приёмника SGN-500, выполненных автором на стоянке в гавани МГУ. Всего было зарегистрировано 204178 значений. Среднее значение ГГФ составило 0,6948. Частоты эмпирического распределения зарегистрированных значений помещены в таблицу 1.

Таблица 1

Частоты распределения величин HDOP приёмника SGN-500 в 2016 году

Величина HDOP	Частота	Относительная частота
0,5	562	0,002753
0,6	63972	0,313315
0,7	96378	0,472029
0,8	33764	0,165366
0,9	7806	0,038231
1	1619	0,007929
1,1	77	0,000377

Из таблицы следует, что на долю значений 0,6 и 0,7 приходится 78,5% всех зарегистрированных величин горизонтального геометрического фактора. Гистограмма распределения HDOP представлена на рис. 4.

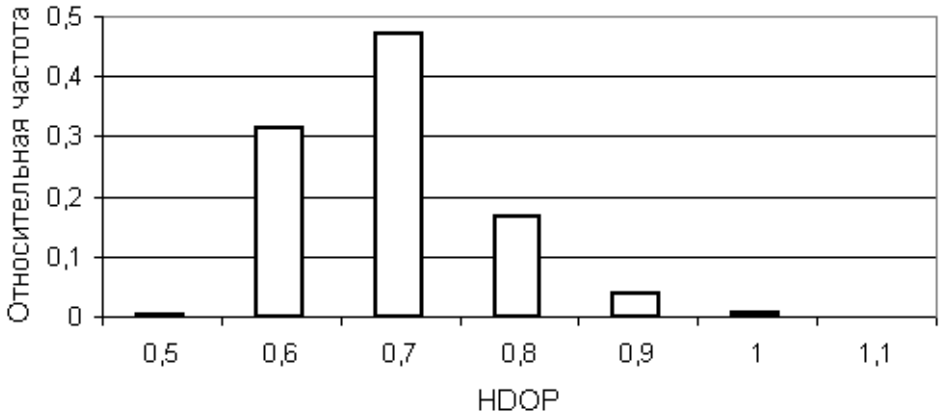

Рис. 4. Гистограмма распределения HDOP приёмника SGN-500 в 2016 году

Анализ гистограммы рис. 4 позволяет утверждать, что эмпирическое распределение величин HDOP приёмника SGN-500 имеет небольшой размах варьирования, что можно воспринять как признак низкой чувствительности этого показателя к изменениям расположения спутников относительно судна. Распределение носит ярко выраженную положительную асимметрию.

Подводя итог, следует остановиться на следующих выводах и предложениях.

1. Величины горизонтального геометрического фактора, вычисляемые судовым СРНС-приёмником SGN-500, вдвое превосходят соответствующие величины приёмника GP-37. Это противоречит свойствам ГГФ, так как приёмник SGN-500 является двухсистемным и принимает сигналы от гораздо большего числа радиовидимых спутников, нежели приёмник GP-37.

2. Несмотря на предсказуемость перемещений спутников относительно судна, характер изменения величин ГГФ приёмника SGN-500 имеет слабо выраженную повторяемость от суток к суткам.

3. Если предположить, что изготовитель волен выбирать алгоритм вычисления HDOP в своей аппаратуре, то такой подход ставит под сомнение полезность горизонтального геометрического фактора для оценки точности определяемых координат. Поэтому сначала надо решить, сохранять его или нет в качестве показателя точности судовых СРНС-приёмников. Если дальнейшее его использование целесообразно, то следует предпри-

нять его широкое обсуждение, чтобы сформировать наиболее приемлемый вид алгоритма вычисления и закрепить этот алгоритм Международной морской организацией для обязательного внедрения всеми изготовителями профессиональной судовой спутниковой аппаратуры.

4. В работе показана низкая чувствительность HDOP приёмника SGN-500 по сравнению с приёмником GP-37. Этот факт позволяет предположить дальнейшее снижение эффективности HDOP в мультисистемной аппаратуре по мере ввода в эксплуатацию СРНС Галилео и Бейдоу.

5. В работе [5] показано, что точность определения координат лучше коррелируется с числом радиовидимых спутников, нежели с величиной горизонтального геометрического фактора. Следовательно, настало время обсудить возможность замены HDOP другим показателем точности. В качестве такового можно предложить контурный показатель точности [6].

Список литературы

1. Комаровский Ю. А. Исследование свойств горизонтального геометрического фактора // Транспортное дело России. Специальный выпуск № 2, Москва, 2004. С. 5-9.

2. Krauter A. Role of Geometry in GPS Positioning. “Periodica Polytechnica Ser. Civ. Eng., 1999, Vol. 43, No. 1, pp 43 – 53.

3. Global Positioning System Standard Positioning Service (SPS) Signal Specification. GPS Navstar, 2nd Edition, June 2, 1995. 98 p.

4. Комаровский Ю. А. Анализ синхронных измерений горизонтального геометрического фактора приёмниками SGN-500 и GP-37 / Теория и практика современного научного знания. Проблемы. Прогнозы. Решения: сборник научн. статей по итогам междунар. научно-практич. конф., г. Санкт-Петербург 19-28 апреля 2017. – СПб: Изд-во КультИнформПресс, 2017. С. 101-105.

5.Комаровский Ю. А. Влияние размера созвездия радиовидимых спутников СРНС Навстар GPS на точность координат потребителя // Проблемы транспорта Дальнего Востока. Пленарные доклады одиннадцатой международной научн.-прак-тич. конф. 2-4 окт. 2015 г. (FEBRAT-15). – Владивосток: ДВО Российской Академии транспорта, 2015. С. 59-63.

6. Комаровский Ю. А. Контурный метод оценки точности ОМС приёмником СРНС Навстар GPS // Вестник Морского государственного университета. Вып. 9. Серия: Судовождение.– Владивосток: Мор. гос. ун-т, 2005. 10-13.

УДК 534.2

Матецкий Владимир Тимофеевич,
старший научный сотрудник лаборатории ЛМИ НОЦ АМИ МГУ им. Г.И. Невельского,
acvatory_1@mail.ru
Прощенко Дмитрий Юрьевич,
к.ф.-м.н., заведующий лабораторией ЛМИ НОЦ АМИ МГУ им. Г.И. Невельского,
alexeyche88@gmail.com
Чехленок Алексей Анатольевич
младший научный сотрудник лаборатории ЛМИ НОЦ АМИ МГУ им. Г.И. Невельского,
dima.prsk@mail.ru

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ПОДАВЛЕНИЯ ВИБРОАКУСТИЧЕСКОГО КАНАЛА УТЕЧКИ ИНФОРМАЦИИ В УПРУГИХ СРЕДАХ

Звуковые волны – переносчики речи, навязчиво демаскируют себя, взаимодействуя на своем пути со всеми веществами обладающими упругостью. Поскольку все газообразные вещества, жидкие и твердые тела упруги, то волна взаимодействует с ними.

В упругих средах, встречающихся на пути, звуковая волна речи возбуждает волны упругой деформации, которые являются звуком той же частоты, но с большей длиной волны, распространяющейся в другой среде. В случае возбуждения вторичных волн в объектах, обладающих большой линейной протяженностью, существует высокая вероятность распространения их на всю длину объекта, как в волноводе. Более того, при наличии плотного примыкания к другому объекту, волна переходит и в него. Такой канал утечки, называемый виброакустическим, является трудно блокируемым и наиболее опасным из-за неконтролируемого распространения виброакустических колебаний далеко за пределы переговорного помещения.

Главная роль в возникновении вибрационного канала утечки принадлежит несущим и ограждающим конструкциям, обособляющим помещение [1]. Обладая большой площадью взаимодействия со звуковыми волнами речи, несущие и ограждающие конструкции получают высокую энергию возбуждения и, как следствие, являются эффективными генераторами виброакустического сигнала утечки речевой информации.

Главными средствами блокирования утечки речевой информации через несущие и ограждающие конструкции помещения являются инженерные средства, направленные на повышение затухания виброзвука за счет увеличения присоединенной колебательной массы, или, как ее принято

именовать в инженерной акустике «поверхностной массы». Современные методы проектирования и строительства, основанные на применении легких, тонких и жестких ограждающих конструкций, в меньшей степени обеспечивают требуемое ослабление звука, чем традиционные, основанные на использовании толстостенных ограждений с большой массой, препятствующей возникновению резонансных колебаний. В случаях недостаточной обеспеченности звукоизоляции ограждения помещений инженерными средствами прибегают к активным методам защиты, основой которых является генерация виброшума при помощи виброизлучателей, с целью ухудшения соотношения сигнал/шум за пределами защищаемой зоны.

Существующие виброизлучатели для зашумления несущих и ограждающих конструкций обладают рядом недостатков, основным из которых является узкополосность излучения и высокая неравномерность частотной характеристики с наличием нескольких резонансов. При активной защите помещений, как правило, спектральные характеристики защитного шума не согласуют со спектральной передаточной функцией ограждения. Такое согласование может повысить эффективность активной защиты.

В архитектурной акустике исследуют спектральные характеристики звукопередачи ограждений в связи с их физическими свойствами и линейными размерами [2]. Здесь определен механизм прохождения звука через ограждающие конструкции, описываемый двумя основными законами – инерционным и резонансным. Собственную звукоизоляцию ограждающей конструкции, то есть без учета косвенной передачи звука, сформулированную еще Лордом Рэлеем, называют законом масс при нормальном падении звука, в соответствии с которым, звукоизоляция равна (дБ):

(1),

где $m = \rho * h$ – масса единицы поверхности (поверхностная плотность кг/м^2); р – плотность материала ограждения, кг/м^3; $\omega = 2nf$ – круговая частота звука, Гц; $\rho_0 c_0$ - удельное акустическое сопротивление воздуха.

Современная модель прохождения звука объединяет в себе закон масс, инерционную и резонансную составляющие. При этом закономерность звукоизоляции ограждений может быть проиллюстрирована графиком на рисунке 1.

В зоне I прохождение звука определяется изгибной жесткостью, здесь также сильно влияние резонансов ограждения. В зоне II звукоизоляция зависит, в основном, от его массы. На участке III сильно влияние волнового совпадения и жесткости. Под волновым совпадением здесь понимают равенство длин проекций падающих под разными углами к поверхности звуковых волнововых фронтов собственным модам изгибных колебаний ограждения.

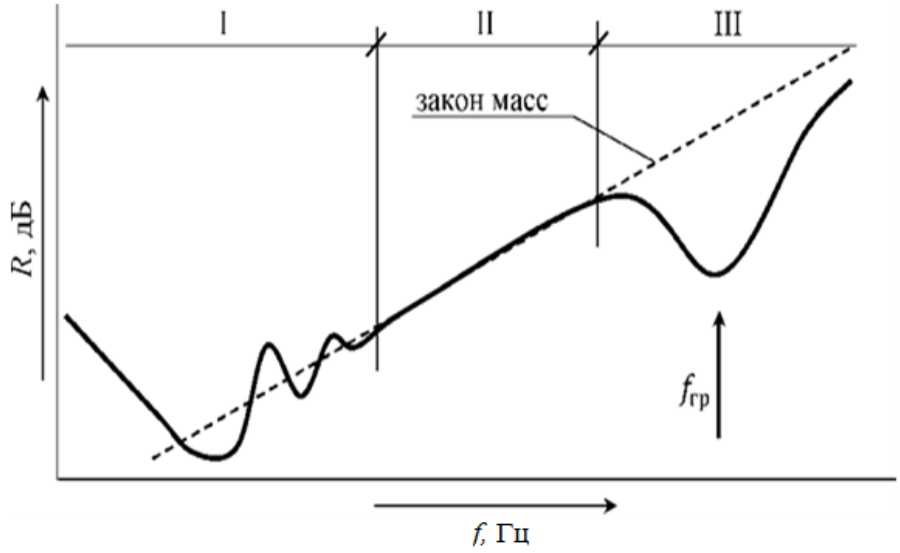

Рис. 1. Закономерность звукоизоляции ограждений

Как было отмечено выше, при использовании современных материалов с малой поверхностной плотностью и высокой добротностью, зона II сжимается, а зоны I и III расширяются. В этой связи все большее значение в передаче виброзвука приобретают резонансные колебания ограждений с частотами, совпадающими с собственными модами. Зона I не несет речевой информации т.к. здесь распространяются виброчастоты до нескольких десятков Герц. Эта зона заполнена структурным сторонним шумом (шум работающих механизмов, удары, звуки шагов и т.п.) Зоны II и III являются областями утечки речевой информации. При малой поверхностной плотности и широком диапазоне частот собственных мод они могут переносить значительную долю энергии виброзвука.

Следствием, вытекающим из рассмотренного механизма прохождения виброзвука, является то, что для эффективного подавления виброакустического канала шумом необходимо учитывать резонансные свойства ограждений, так как существует опасность утечки информации на резонансах, соответствующих собственным модам ограждения. Ограждающую конструкцию можно представить в виде многомодовой колебательной системы, подобной гребенчатому фильтру. Тогда виброакустический сигнал, распространяющийся в конструкции $S_{ва}(\imath\omega)$, является результатом перемножения спектра речевого сигнала $S_{г}(\imath\omega_{г})$ на амплитудно-частотную характеристику этого фильтра $S_{к}(\imath\omega_{к})$.

Для проверки вывода о модовой структуре был проведен эксперимент на моделях ограждений. В качестве моделей использовались образцы акустически высокодобротного материала - однородного (стекло) и композтного (плоский шифер). Образцы прямоугольной формы зажимались по периметру в жесткой рамке. В качестве тестового сигнала был применен генератор на основе лазерного возбудителя термоупругового звука. Виброакустический сигнал, генерируемый таким способом, имеет спектральную

полосу более 100 мГц, что позволяет считать его, в рамках решаемой задачи, идеальным для получения амплитудно-частотной характеристики модели ограждения. В качестве приемника виброзвука применялась пьезокерамика с частотой собственного резонанса 10 мГц, подключенная к широкополосному усилителю.

На рисунке 2 приведен пример записи виброакустического сигнала, полученного на модели из шифера при совпадении осей излучения и приема.

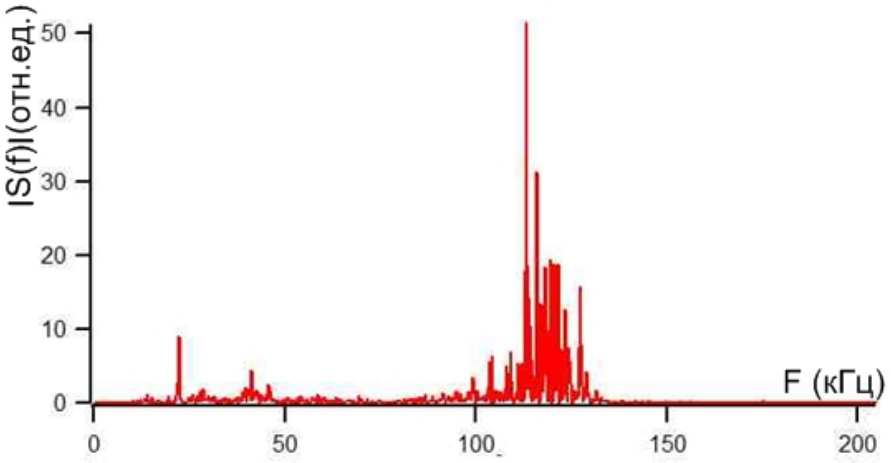

Рис. 2. Пример записи виброакустического сигнала,
полученного на модели из шифера при совпадении осей излучения и приема

Из рисунка видно, что основная энергия в этом случае сосредоточена в области высоких акустических частот, так как передаточная функция мишени оказывает малое влияние. Спектральные линии в нижней части диапазона – частоты, возбужденные на резонансах мишени. При смещении пьезокерамического датчика в сторону от оптической оси передаточная спектральная характеристика мишени оказывает большее влияние, которое сказывается на подавлении высоких частот и выделения низкочастотной резонансной области. На рисунке 3 приведен пример записи спектральной плотности такого сигнала.

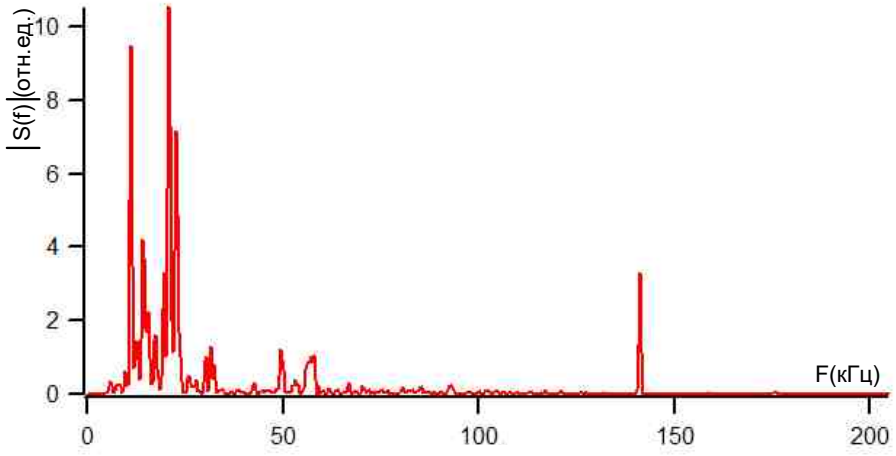

Рис. 3. Пример записи спектральной плотности сигнала,

полученного на модели из шифера при разнесении осей излучения и приема

На рисунке 4 приведен пример записи спектральной плотности сигнала, полученного на модели из стекла при разнесении осей излучения и приема.

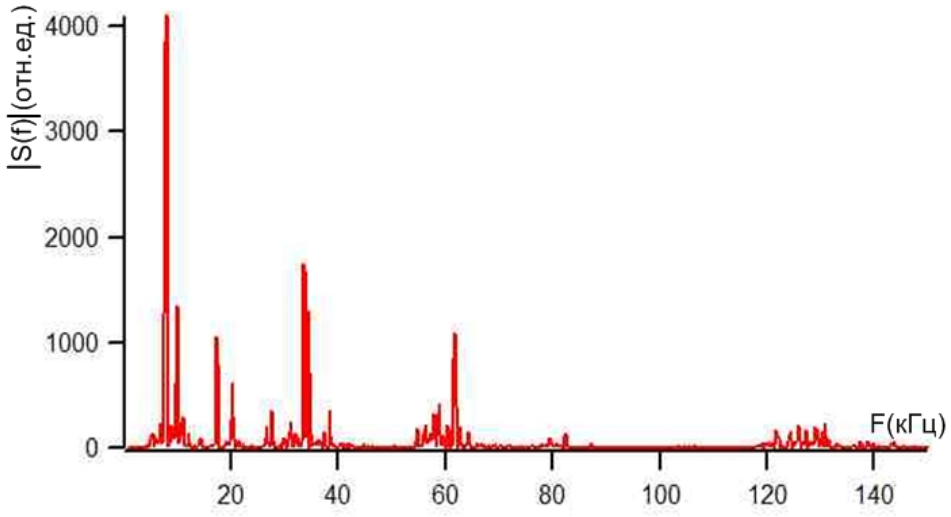

Рис. 4 Пример записи спектральной плотности сигнала, полученного на модели из стекла при разнесении осей излучения и приема

Здесь четко проявила себя модовая структура передаточной функции мишени с характерным спадом энергии в область повышения частот. Следует отметить, что столь явное уменьшение энергии в область высоких частот наблюдалась только на стеклянной мишени, которая характеризуется высокой добротностью.

Проведенный эксперимент показывает, что для повышения эффективности подавления виброакустического канала утечки информации требуется сигнал зашумления, согласованный спектрально с передаточной функцией ограждения. При звестной передаточной характеристике ограждения и виброакустического излучателя можно при помощи обратного преобразования Фурье произведения этих функций получить вид требуемого сигнала подавления во временной области, согласованного с ограждающей конструкцией.

Список литературы

1. Бузов Г. А. Защита от утечки информации по техническим каналам: Учебное пособие / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. – М.: Горячая линия – Телеком, 2005. – 416 с.

2. Бобылев, В.Н. Изоляция воздушного шума однослойными ограждающими конструкциями [Текст]: учеб. пособие / В.Н. Бобылев, В.А. Тишков, Д.В. Монич. – Нижегород. гос. архитектур.-строит. ун-т. – Н. Новгород: ННГАСУ, 2014. – 67 с.

УДК 004(075.8)

Павликов Сергей Николаевич,
к.т.н., зав. каф. РЭРС, профессор, МГУ им. адм. Г.И. Невельского
Коломеец Валерия Николаевна,
аспирант 1 курса ВГУЭС
Динкилакер Виталий Викторович,
аспирант 1 курса ВГУЭС
Степанушкин Леонид Викторович,
аспирант 1 курса ВГУЭС

АНТИВИРУСНАЯ СЕТЬ

Информационные сети являются объектами изучения и нападения противником. Деструктивные действия противной стороны могут привести к возникновению чрезвычайных ситуаций с последствиями в виде материальных и информационных и др. потерь. Задача обеспечения безопасности таких объектов является важнейшей. Эффективность систем защиты зависит от качества поставленной задачи, информационного обеспечения и методов их обработки. При проектировании средств защиты (СЗ) самыми сложными являются методика анализа защищенности объекта, новизна технического решения и рекомендаций по выбор варианта и технологий настройки и адаптации СЗ в течение эксплуатации. Как показывает, практика ситуация технологий «защиты и нападения» постоянно меняется. При этом надежного, гарантированного варианта защиты не существует. Все известные антивирусные программы имеют как положительные, так и отрицательные свойства. При проектировании СЗ специалисты могут только прогнозировать большую часть входных данных. В данной работе предлагаются новая структура СЗ и модель оценки защищенности объекта от вирусных угроз [1]. Рассмотрим процесс экранирования информационной сети. Экран – это средство разграничения доступа между внутренней и внешней сетями. Контроль потоков состоит в их фильтрации, возможно, с выполнением некоторых преобразований. Каждый из фильтров, выполняющих различные преобразования, могут пропустить или задержать программный входной продукт. Помимо функций разграничения доступа, экраны осуществляют протоколирование обмена информацией. Обычно экран не является симметричным, для него определены понятия "внутри" и "снаружи". При этом задача экранирования формулируется как защита внутренней сети от потенциально враждебной внешней, а также возможность контролировать информационные потоки,

направленные во внешнюю область, что способствует поддержанию режима конфиденциальности в информационной сети (ИС) предприятия. Таким образом, реализуются принципы эшелонированности, ассиметричности, управляемости, аудита, адаптации, скрытность защищаемой сети и др.[2]. Сформулируем задачу построения СЗ следующим образом: необходимо разработать весь спектр возможных технических решений по заданному критерию, выбрать новые технологии, согласовать их с существующими и обосновать наилучший вариант реализации СЗ с последующим подтверждением в ходе имитационного моделирования. Критерием эффективности СЗ является уровень защищенности, выраженной через вероятность его защиты, при допустимых затратах на угрозы информационной системы. Вероятность защиты объекта $P_з$ зависит от возможных угроз и средств защиты и может быть представлена в виде сложного события, состоящего из этапов приведенных в таблице 1[3]. Таким образом, эффективность СЗ в общем виде определяется степенью оснащенности антивирусными программами и адекватности их различным атакам. Предлагается СЗ построить по принципу антивирусной сети в виде матрицы в узлах которой расположены различные антивирусные программы с возможностью построения траекторий каналов через трассы по данной матрице. Выбор оптимальных вариантов управления каналами антивирусной сети для увеличения пропускной способности может осуществляться единой (пространственно разнесенной) комплексной системой, выбирающей в зависимости от условий антивирусные программы в последовательно-параллельном разделения каналов и оптимизирующий использование ресурсов антивирусной сети.

Таблица 1

Компоненты оценки эффективности элементов антивирусной сети

№ индекса	**Название показателей этапов противоборства**	**Условные обозначения**
1.	Вероятность своевременного обнаружения нападения	P_1
2.	Вероятности оценки распознавания атаки	P_2
3.	Вероятность задержки вредоносной программы	P_3
4.	Вероятность нейтрализации нарушителей	P_4

На рисунке 1 представлен принцип формирования антивирусной сети путем построения необходимого количества параллельных, но с различным сочетанием антивирусных программ каналов, за счет расширения пространства их разделения и сочетания для решения различных по сложности угроз ИС [3]. По оси ординат указываются типы антивирусные программы, по горизонтали - время (последовательность процедур проверки

входного сообщения различными антивирусными программами). Линии графиков указывают траектории выбранных антивирусных программ. Метод антивирусной сети повышает пропускную способность, а также повышает вероятность защищенности за счет сочетаний применения антивирусных программ в пространстве и во времени.

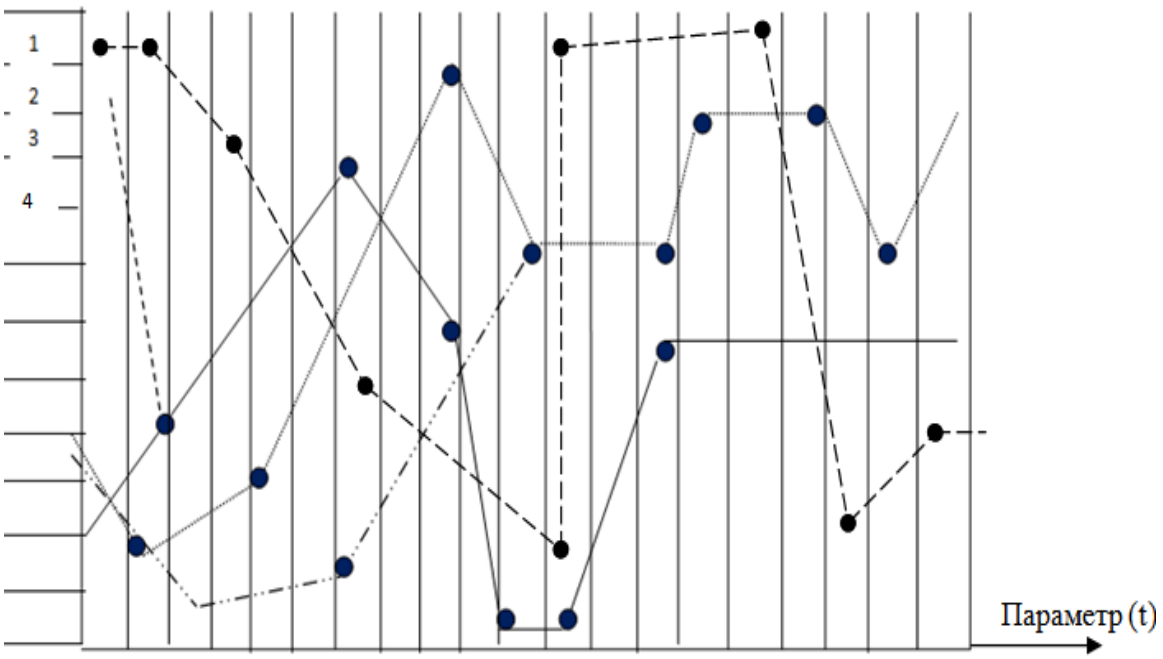

Рис. 1. Принцип формирования антивирусной сети

Комплексный анализ результатов антивирусной проверки входных информационных потоков позволяет повысить вероятность обнаружения, классификации и ликвидации вирусной программы. Статистический анализ позволяет антивирусной сети накапливать результаты работы различных антивирусных программ (АВП) с определением эффективности для различных атак и расчетом коэффициента значимости для типовых вирусов при различных условиях и ограничениях. Результаты статистического анализа используются по цепям обратных связей для ранжирования АВП и их весов при коллективном принятии решений в узлах и на выходе сети. Вариант структурной схема устройства приведена на рисунке 2.

Таким образом, предложено новое техническое решение построения сетевого экрана с использованием принципов эшелонированности, ассиметричности, управляемости, аудита и адаптации антивирусной сети, обеспечивших достижение скрытность защищаемой сети, повышенной надежности обнаружения и классификации вредоносного продукта, а также с повышенной пропускной способностью.

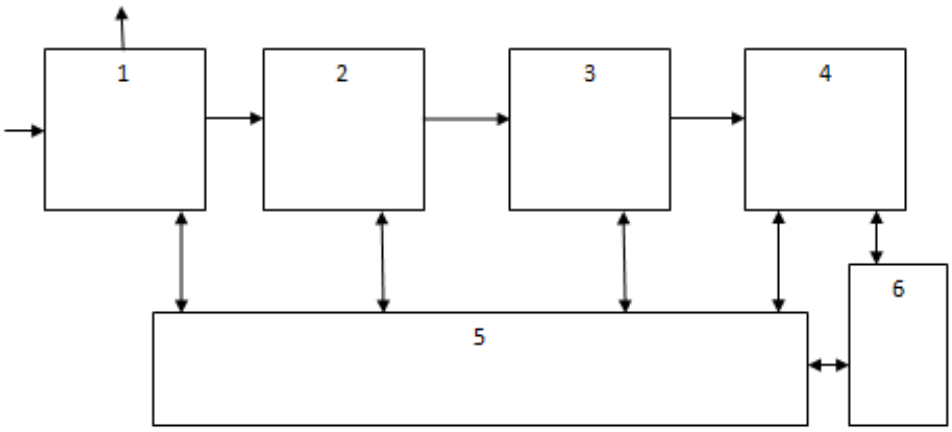

Рис. 2. Принцип формирования антивирусной сети, где обозначены: 1 – входной коммутатор; 2 – многоканальная матрица; 3 - блок весовой обработки; 4 – вычислительный блок принятия решения; 5 – блок управления

Список литературы

1. Панин О.А. Как измерить эффективность? Логико-вероятностное моделирование в задачах оценки систем физической защиты / Безопасность – Достоверность – Информация. 2008. №2(77). с. 20-24.
2. Радаев Н.Н. Приближенные оценки защищенности объектов от террористических действий / Безопасность – Достоверность – Информация. 2007. №3(72). с. 28-32.
3. Павликов С.Н. Спутниковые технологии в обеспечении безопасности мореплавания [Текст]: монография / Павликов С.Н., Веселова С.С. – Владивосток: Мор. гос. ун-т, 2012. – 165 с.

УДК 621.39

Павликов Сергей Николаевич,
к.т.н., зав. каф. РЭРС, профессор, МГУ им. адм. Г.И. Невельского
Убанкин Евгений Иванович,
к.т.н., доцент кафедры РЭРС, доцент, МГУ им. адм. Г.И. Невельского
Цепелева Алёна Сергеевна,
аспирант 1 курса МГУ им. адм. Г.И. Невельского
Пленник Милена Денисовна,
аспирант 1 курса МГУ им. адм. Г.И. Невельского

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТА НА МОРЕ

В работе исследованы методы и технологии обеспечения безопасности от угроз для судна. Количество угроз постоянно возрастает, поэтому необходимо разработать общую теорию обеспечения безопасности. Предлагается обобщенная математическая модель обеспечения безопасности, включающая следующие компоненты: множество объектов **Ω** и элементы

ω_i объектов, $j = \overline{1, M}$ с формуляром $\vec{\Lambda}$ параметров состояний и характеристиками функционирования; множество угроз безопасности Y и K – технологий (способов и устройств) реализации воздействий, приводящих к снижению безопасности элементов объекта; множество методов Z обеспечения безопасности по противодействию (защите от угроз) угрозам; множество технических L методов обеспечения безопасности элементов объекта от угроз; множество методов оценки эффективности $Э$ технологий обеспечения безопасности элементов и объекта в целом. пространство оценок стоимости технических средств и методов обеспечения безопасности C от K – технологий реализации Y угрозы; пространство $Д$ решений по обеспечению безопасности элемента объекта ω_i и объекта Ω в целом; база данных (БД) обеспечения безопасности объекта. Под множеством ω_i элементов объекта Ω будем рассматривать компоненты математической модели объекта, требующие защиты (имеющие ответственное назначение). Для судна элементами ω_i являются: технические средства; груз; экипаж и пассажиры и информация. Элементы представляют собой множество, требующее защиты от угроз и дестабилизирующих факторов. Данные элементы имеют определенное назначение, массогабаритные и др. характеристики $\vec{\Lambda}_a(\omega_i)$, описывающие ценность – a_1 и значимость – a_2 элементов для безопасности судна и базовый уровень защиты – a_3 от дестабилизирующих факторов, таких как давление, температура, влажность и т.д. В работах [1, 2] описаны основные угрозы безопасности элементов объекта (судна) и выделены в отдельное множество (пространство). Отображение элементов (точек) пространства угроз Y в точки пространства элементов ω_i объекта проявляется в виде потенциальной угрозы или угрозы реализованной с вероятностными характеристиками $P_{\text{пот.}Y}$ или $P_{\text{реал.}Y}$ соответственно. Методы реализации угроз составляют свое случайное множество K реализуемых воздействий угрозы Y на элемент ω_i объекта. Условная вероятность реализуемого K воздействия источника Y угроз K-методом обозначим $P(Y_k/\omega_i)$, а $P(Y/\omega_i)$ – условная вероятность воздействия угрозы Y всеми K методами воздействий на ω_i; $P(Y_K/\Omega)$ – условная вероятность реализации K-воздействия на весь объект Ω. Множество методов Z обеспечения безопасности приведены и описаны в первом разделе. В работе рассмотрен поиск технологии в пределах множества L технических методов и средств обеспечения безопасности ω_i и Ω в целом. В состав технологий L входят: методы LN наблюдения за наличием и реализацией K способов воздействия из пространства Y угроз; методы построения модели LM оценки степени опасности угроз Y; методы LP прогнозирование событий и оценки потенциальных потерь безопасности ω_i в виде снижения параметров и ухудшение характеристик $\vec{\Lambda}_a(\omega_i)$ у элементов объекта Ω; технические методы обеспечения безопасности LZ. Методы LZ обеспечения безопасности включают процессы отображения множества точек методов K реализации угроз Y на элементы ω_i через

фильтр, реализующий защиту *l*-методом. Обозначим процедуру обеспечения безопасности $LZ(l,YK,Y,\omega_i)$, подразумевая, что использует *l*-метод обеспечения безопасности (защиты) от воздействия *Y* угрозы *K*-методом на элемент ω_i. Пространство методов оценки эффективности техническими технологиями обеспечения безопасности элементов объекта может быть представлена функционалом $Э[LZ(l,YK,Y,\Omega_i)]$ – эффективность того, что *K*-метод реализации *Y* угрозы безопасности *i* элементу **Ω** объекта будет устранен методом *l*. В роли $Э[LZ(l,YK,Y,\Omega)]$ может быть использован критериальный параметр – вероятность того, что *Y* – угроза (реализуется методом *K*) объекту **Ω** будет снижена до допустимого значения $P(Y_k/\Omega) \le P_{доп}$, при стоимости соответствующей условию $C \le C_{доп}$. Методы обеспечения безопасности приводят к использованию необходимых ресурсов. Стоимость обеспечения безопасности угрозы имеет большое практическое значение в сравнении со стоимостью элементов и самого объекта, подлежащего защите. Под стоимостью средств защиты подразумевают затраты (финансы) в течение всего жизненного цикла. Пространство оценок стоимости методов и средств обеспечения безопасности (противодействия угрозам) от угроз соответствует значениям стоимости конкретных средств *LZ* на этапах проектирования производства, установки, обслуживания, применения, анализа результатов, модернизации и т.д. вплоть до утилизации. При рассмотрении далее ограничимся стоимостью конкретных средств *LZ*, приведенного к моменту его применения. Обозначим $C(l,YK,Y,\omega_i)$ – как стоимость *l*-технологии обеспечения безопасности элемента ω_i объекта от *K*-метода нападения *Y* угрозы. Угрожающая сторона оценивает стоимость формирования потенциальной угрозы и ее реализацию неким функционалом: $CY(YK,\omega_i,Z,L)$ – стоимость реализации нападения методом *K* на элемент ω_i объекта, предполагается, что объект защищен методом *Z*. $CY(K,\Omega,Z,L)$ – стоимость реализации нападения с помощью технологии *K* на объект **Ω**, предполагается, что объект защищен методом *Z*, в том числе техническим методом и средствами *L*. Нападающая сторона, в свою очередь также оценивает эффективность применения тех или иных технологий *K* для реализации угрозы *Y* на объект **Ω** или его элементы ω_i. Обозначим такую оценку в виде $ЭY(YK,\omega_i,LZ)$ – как эффективность применения технологии *YK* угрозы *Y* по элементу ω_i объекта, предполагается, что объект использует *Z* технологию обеспечения безопасности. В состав *Z* входят технические методы *L*, которые включают, как правило, составляющие: *LN*, *LM*, *LP* и *LZ*. Пространство решений *Д* представляет собой комплекс частных решений по обеспечению гарантированной безопасности объекта и его элементов от угроз при заданных условиях и ограничениях. Алгоритм решения *Д* осуществляет отображение угроз *Y*, *K*-методами, на элементы ω_i объекта **Ω** в пространствах **Ω**, ω_i, *Y*, *K*, *Z*, *L*, *Э*, *C*, *ЭУ*, *CY*, *ДУ*. Структурная схема такого взаимодействия приведена на рисунке 2.18 и представляет собой графическое представление общей математической модели обеспечения безопасности объекта. На решение БД включает

априорные данные обо всех компонентах, входящих в общую математическую модель обеспечения безопасности объекта. Решающий функционал ω_i является ключевым звеном общей математической модели, осуществляющим управление доступными методами характеристик и свойств компонентов модели для гарантированного обеспечения требуемого уровня безопасности объекта. Работа функционала *Д* заключается в выработке решающей функции *d* для достижения поставленной цели. Обобщенная математическая модель обеспечения безопасности объекта представлена выражением:

$$Э[Д[Z\{L(LZ\{Y(\Omega(\omega_i))\})\}]] \geq Э_{зад\Omega}, \; Э[Д] \geq ЭY[ДY],$$
$$LZ(l, YK, Y, i) \geq LZi_{доп}^{\min}, C(l, YK, Y, i) \geq Ci_{доп},$$
$$LZ(l, YK, Y, \Omega) = \sum LZ(l, YK, Y, i) > LZ\Omega_{доп}^{\min}, \; C(l, YK, Y, \Omega) \geq C_{\Omega доп}.$$

Общая математическая модель представляет собой систему оптимизационных задач при заданных условиях и ограничениях. Процесс оптимизации каждой из них может быть представлен в виде $d = extrem\{(\bullet)\}$, где (●) векторов параметр из рассмотренных ранее множеств *Y*, *K*, *Z*, *L*, *Э*, *C* при заданной БД.

Решающая функция определяет параметры технологий обеспечения безопасности для: минимизации угроз *Y* и методов их реализации *K*; минимизации стоимости технологий обеспечения безопасности объекта; максимизации эффективности обеспечения безопасности объекта; минимизации технологий, обеспечивающих достижимый уровень безопасности объекта. Обобщенная структурная схема математической модели обеспечения безопасности представлена на рисунке 1.

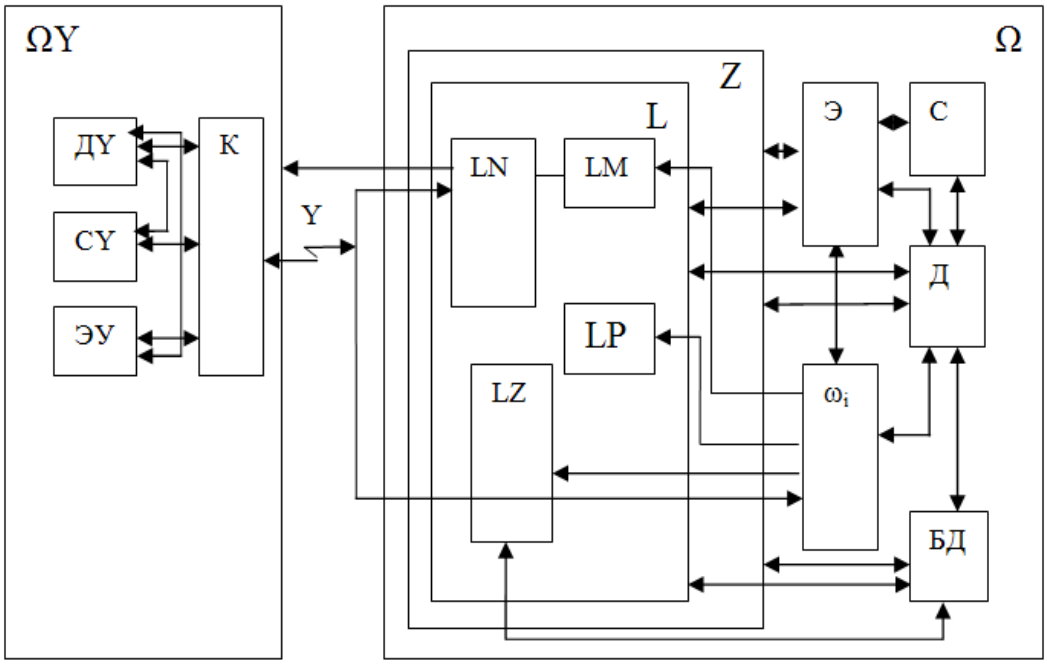

Рис. 1. Обобщенная структурная схема математической модели

обеспечения безопасности

Один из вариантов математической модели представлен функционалом:

$$d = \max\{Д[D[Z\{L(LN,LM,LP,LZ)\{Y(\Omega(\omega_i))\}\}]]\},$$

при $C \le C_{доп}$; $Z \ge Z_{min}$; $CY \le CY_{доп}$; $T \le T_{доп}$; $L \ge L_{min}$; $ЭY \le ЭY_{доп}$;

$DY(P_{пот.Y} \ge P_{доп.пот.Y}$; $P_{реал.Y} \ge P_{доп.реал.Y})$.

Алгоритм работы математической модели решающей функции d приведен на рисунке 2 и включает следующие процедуры:

1. Постановка задачи на моделирование с описанием сценария и компонентов:

1.1. Y угроз;

1.2. K технологий (нападения) воздействия

1.3. Ω объекта защиты с его характеристиками;

1.4. ω элементов объекта с характеристиками;

1.5. Z уровень методов обеспечения безопасности объекта (ОБО);

1.6. L технических методов и устройств ОБО с описанием характеристик его компонентов; 1.6.1. LN; 1.6.2. LM; 1.6.3. LP; 1.6.4. LZ;

1.7. C – матрица оценок средств обеспечения безопасности и элементов ω_i объекта;

1.8. $Э$ – методики оценки эффективности;

1.9. БД – базе данных с характеристиками условий и ограничений на параметры по компонентам модели: $Э$, C, T;

1.10. временные ограничения работы модели;

1.11. условия завершения моделирования;

1.12. формуляр исходных данных и результатов моделирования;

1.13. прогнозируемый уровень информации объекта Ω об угрозе и информации объекта носителя угроз о параметрах объекта и степени защищенности $\dot{\Lambda}(\omega_i)$ его элементов.

2. Задается уровень объекта обеспечения безопасности:

2.1. элемент ω_i;

2.2. группа взаимосвязанных элементов ω_i;

2.3. группа не связанных друг с другом элементов ω_i, ω_j;

2.4. объект Ω.

3. Задаются уровни защиты:

3.1. a_{3i} − технологии базового уровня обеспечения безопасности элемента ω_i;

3.2. $a_{3\Omega}$ − технологии базового уровня обеспечения безопасности объекта.

4. Временной масштаб моделирования m_t.

5. Формирование или выбор из БД сценария работы математической модели, ее компонентов и критериальной системы технологий обеспечения безопасности объекта.

6. Уточнение модели *LM*.

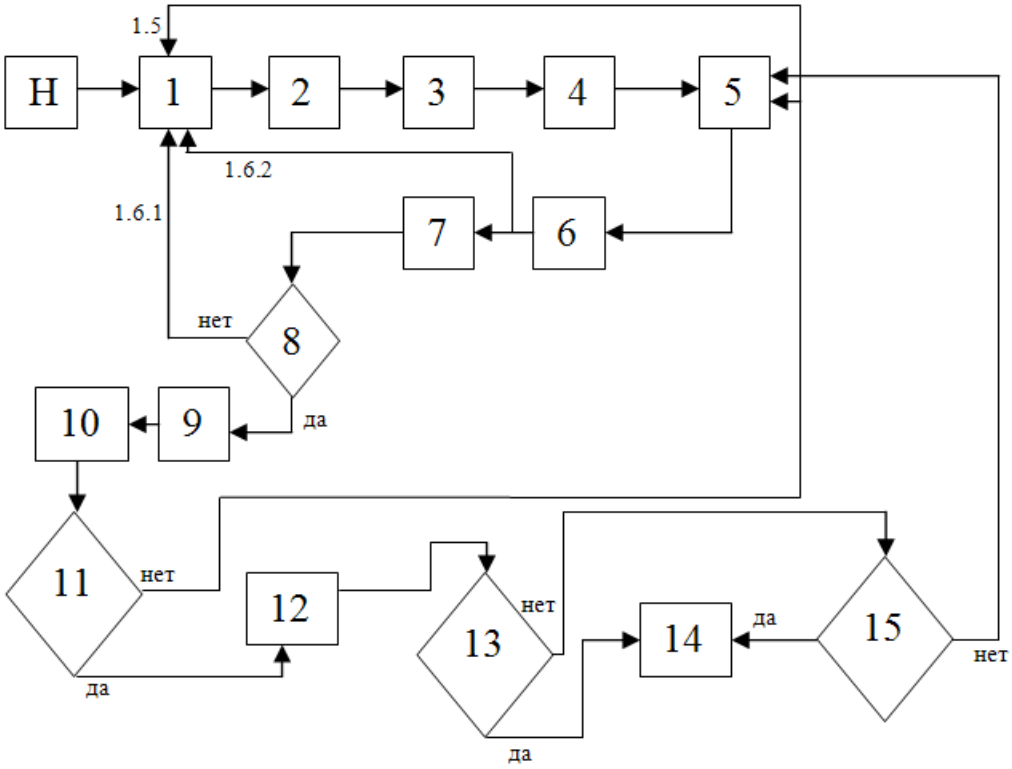

Рис. 2. Алгоритм работы математической модели

7. Прогнозирование *LP* степени угрозы.

8. Проверка условий достаточно ли информации для работы модели, иначе подключение модуля *LN* за угрозами *Y* и реализуемыми технологиями нападения *K*.

9. Оценки степени соответствия базового уровня защиты $\dot{\Lambda}(\omega_i)$ элементов объекта угрозам *YK*.

10. Оценка стоимости технологий обеспечения безопасности элементов и объекта в целом.

11. Проверка условия $YK \geq a_{3i}$, $YK \geq a_{3\Omega}$ и $C_{LZ} \geq C_{\underset{LZ}{доп}}$. Если хотя бы одно условие не выполняется, то изменение уровня *Z* в п.1.5 и переход к п.5.

12. Разработка решения d_i или d_i, d_j или d для соответствующего уровня обеспечения безопасности элемента i или элементов $i, j\ldots$ или объема в целом. Формирование формуляра решения: *d*.

13. Анализ соответствия условий завершения моделирования: если нет, то 15, иначе 14.

14. Конец.

15. Наблюдение *LN* за изменением угроз и состояний элементов ω_i объекта. Проверка условий если изменения незначима ($\Delta \leq \Delta_{доп.}$), то переход к п. 14, иначе переход к п. 5.

Перечисленные технологии позволяют управлять качественными параметрами систем связи, повышая своевременность, достоверность и точность в широком диапазоне значений, что в итоге повышает эффектив-

ность системы обеспечения безопасности объектов на море. Разработанные технологии могут использоваться не только в спутниковых системах связи, но и адаптироваться к другим приложениям.

Однако именно в спутниковых средствах связи, предназначенных для обеспечения безопасности на море, предлагаемые технические решения наиболее значимы в условиях быстро нарастающих угроз.

Список литературы

1. Перспективы развития системы радиосвязи нового поколения / Павликов С. Н., Веселова С. С., Раудин А. Л., Цымбал И. В. // Вестник Морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2010. – Вып. 43. – С.140–143.

2. Основные направления совершенствования радиоэлектронных систем / Веселова С.С. // Сборник докладов 58-й международной молодежной научно-технической конференции «МОЛОДЕЖЬ-НАУКА-ИННОВАЦИИ», 24–25 ноября 2010 г. в 2 т. – Владивосток: Мор.гос.ун-т, 2010. – Т.1. – С.66–70.

УДК 004.052.2

Патенкова Анастасия Петровна,
студентка 1-го курса, МГУ им. адм. Г.И.Невельского,
Щербинина Инна Александровна,
к. пед. н., декан ФТФ, МГУ им. адм. Г.И.Невельского, shcherb-inina@msun.ru

ОБЗОР СУЩЕСТВУЮЩИХ ТЕХНОЛОГИЙ ПРИМЕНЕНИЯ БЕСКОНТАКТНЫХ КАРТ

Бесконтактные смарт-карты (от англ. smart card) представляют собой пластиковые карты со встроенной микросхемой. Микросхема содержат микропроцессор и операционную систему, которые контролируют доступ к объектам в памяти карты. Бесконтактные карты не содержат встроенного источника питания. Для обмена данными используется RFID-технология (от англ. Radio Frequency Identification – радиочастотная идентификация). Сегодня бесконтактные карты используются и как средство ограничения доступа, так и средство платежей.

Для расчёта бесконтактной банковской картой необходимо приложить или поднести «пластик» к считывающему устройству терминала. Проведение операции не требует ни введения ПИН-кода, ни подписи на чеке. Максимальная сумма транзакции всегда ограничена – по картам российских банков она составляет 1 тыс. рублей.

В отличие от обычных магнитных и чиповых карт «пластик» с бесконтактной технологией оплаты не хранит сведения о CVV коде. Для каж-

дой последующей операции формируется динамический одноразовый CVV.

Бесконтактный «пластик» более безопасен чем магнитная карта, но уступает в данном вопросе платёжным инструментам, содержащим только обычный чип. Например, в прошлом году у россиян, использующих карты payWave и PayPass было украдено 2 млн рублей. С помощью самодельных RFID-ридеров, мошенники считывали с карт посетителей торговых центров динамический CVV, а затем создавали их клоны и рассчитывались ими в ближайшее время в магазинах. Спустя некоторое время, когда владелец «пластика» пытался оплатить им покупку, система, обнаружив, что CVV уже использовали ранее, блокировала доступ к карточному счёту, но к этому времени на нём уже недоставало денег [1].

Как указывает замдиректора департамента аудита защищённости компании Digital Security Глеб Чербов, мошенникам достаточно бесконтактно получить номер карты и дату окончания срока её обслуживания. Этого хватит для проведения транзакций через подставные интернет-площадки или изготовления дубликата магнитной полосы карты. «Из доступной «по воздуху» информации для злоумышленников также представляет интерес история операций по карте, включающая в себя точные суммы и даты списаний. Располагая этими данными, несложно составить примерный профиль владельца и предположить текущий остаток по счёту», – отмечает IT-эксперт[2].

Среди преимуществ бесконтактных карт перед другими видами можно обозначить:

– надёжность карты доступа, сочетающаяся с длительным сроком её эксплуатации из-за отсутствия физического контакта со считывателем; магнитные карты доступа и иные аналоги предусматривают физическое взаимодействие со считывателем, что приводит к быстрому износу;

– возможность перезаписи информации (до 100 000 раз);

– разнообразие областей применения – от электронной подписи до средства платежа;

– высокая скорость передачи данных с/на считыватель;

– длительное время хранения информации, из-за невосприимчивости к воздействию внешних полей информация может храниться на карте до 10 лет;

– высокая защищённость от подделки (в отличие от магнитной карты доступа, или карты со штрих кодом, бесконтактная карта практически исключает возможность подделки).

По принципу действия бесконтактные карты делятся на три категории:

– R/W (Read and Write) – допустимы многократное чтение и многократная запись;

– WO/RM (Write Once / Read Many) – многократное считывание и

лишь однократная запись;

– R/O (Read Only) разрешено только считывание.

По частоте используемых радиосигналов, протоколам обмена, объёмам информации на карте и типам используемой модуляции можно выделить три основных диапазона частот, используемых в бесконтактных картах:

– низкочастотные – от 100 до 500 КГц;любая смарт-карта, использующая данную частоту, позволяет считывать данные на расстоянии 5-30 сантиметров;при применении данных частот приходится использовать достаточно большую антенну, что ограничивает сферу использования карт доступа;наиболее распространены системы, использующие частоту 125 КГц, и работающие с протоколом швейцарской фирмы EM-Marin производители смарт-карт;к этой группе бесконтактных пластиковых карт относится бесконтактная смарт-карта ISO EM-Marin;

– среднечастотные –10-15 МГц;эта группа отличается от предыдущей меньшими габаритами антенны, а также большей дальностью считывания;высокая скорость считывания данных, обеспеченная более высокой частотой работы, позволяет использовать транспортеры типа Read/Write, функционирующие в диапазоне частот 13,56 МГц, БСК-смарт-карт;за счёт возможности изготовления небольших по своим габаритам идентификаторов, выделяющихся низкой себестоимостью, данная группа получила наибольшее распространение на сегодняшний день; рассматриваемая группа обладает более высокой скоростью считывания информации, за счёт чего считыватель имеет возможность обрабатывать данные с нескольких карт одновременно;несмотря на то, что данный диапазон подвержен воздействию промышленных электромагнитных помех, рассматриваемые системы весьма популярны в БСК Proximity в системах контроля доступа;

– высокочастотные (850-950 МГц и 2,4-5 ГГц) – смарт-карты данной группы отличаются большим радиусом зоны действия (считывание может производиться на расстоянии 10-15 метров), а также высокой скоростью считывания данных; этого удаётся достичь за счёт применения остронаправленных антенн считывателей, а также более высоких мощностей запросного сигнала; данная особенность формирует и иные отличительные черты высокочастотных систем; бесконтактные карты рассматриваемой группы стоят намного дороже, нежели магнитные карты доступа или карты из двух вышеописанных групп.

Электронная схема бесконтактной карты включает в себя smart-чип и антенну (рис. 1). Антенна карточки выполнена в виде печатных проводников, а smart-чип объединяет приёмник, передатчик и энергонезависимую, электрически перепрограммируемую память для хранения кодов доступа и дополнительной информации. Идентификация объекта производится циф-

ровому коду, хранимому в памяти smart-чипа и излучаемому в диапазоне радиоволн.

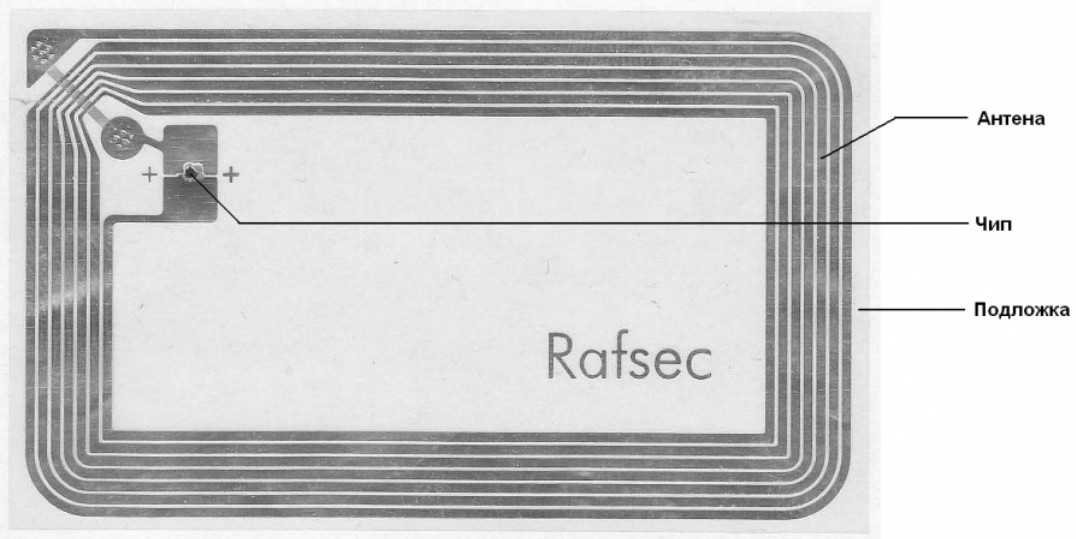

Рис. 1. Электронная схема бесконтактной карты

Опрос бесконтактных пластиковых карт производится автоматически с помощью приёмо-передающего устройства (считывателя). Карта получает сигнал от считывателя и формирует ответный сигнал, который принимается антенной считывателя, обрабатывается его электронным блоком и по интерфейсу направляется в компьютер, для принятия какого либо решения.

Энергию, необходимую для формирования ответного сигнала, карты получают по радиоканалу от считывателя. Обмен данными ведётся по зашифрованному протоколу, доступ к памяти возможен только по предъявлении секретных ключей, которые хранятся в модуле безопасности терминала и не могут быть прочитаны из него. Ключи назначаются эмитентом, что гарантирует их защиту от изготовителя карты и разработчика платежной схемы.

Пара «карта–считыватель» работает следующим образом (рис. 2). Считыватель содержит генератор, который запитывает антенну считывателя. Излучаемая антенной считывателя энергия принимается антенной карты и используется для питания микросхемы (чип), которая при появлении питания с помощью модулятора (М) начинает модулировать сигнал считывателя кодом, записанным в постоянном запоминающем устройстве (ПЗУ) карты. Модулированный сигнал в считывателе детектируется, усиливается и поступает на микроконтроллер, который преобразует принятый от смарт-карты сигнал к виду, удобному для передачи на внешнее устройство, к которому подключён считыватель. Считыватели бесконтактных

карт подключаются к контроллерам доступа, используются для чтения номера карты и передачи его в контроллер [3].

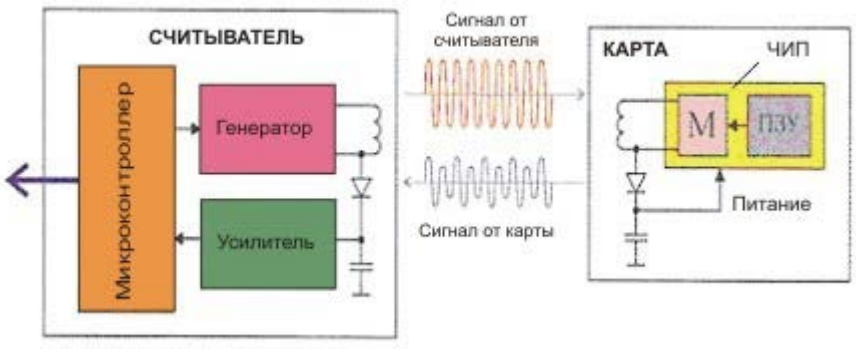

Рис. 2. Принцип работы электронной карты

Самым распространённым интерфейсом между ридерами и контроллерами в системах контроля доступа, безопасности, и др. смежных областях является Wiegand. Стандарт Wiegand принят как базовый для соединения считывателей и контроллеров в системах безопасности, что обеспечивает совместимость и взаимозаменяемость элементов.

Протокол Wiegand, созданный как экономичное средство выдачи данных с карты доступа, информация с которой считывается с помощью картридера. На данный момент фактически каждый производитель картридеров ориентируется на протокол Wiegand. Он используется и для Proximity-считывателей, и для Smart-считывателей, и для кодонаборных панелей и устройств на базе биометрических технологий.

Стандарт применительно к сигналу предполагает использование двух линий данных для передачи сигнала считываемого с карточки к контроллеру. Они называются data1 и data0. Линия, именуемая data1, служит для передачи битов «1» из данных передающихся на контроллер. Линия, именуемая data0, служит для передачи битов «0» от считывателя к контроллеру. В обоих случаях амплитуда сигнала в линии изменяется от 5В до 0В.К недостаткам интерфейса следует отнести то, что он не поддерживает шифрование передаваемых данных, аутентификацию сторон, контроль целостности линии между считывателем и контроллером.

Другим интерфейсом, используемым в бесконтактных картах, является интерфейс 1-Wire (Dallas Touch Memory), разработанный фирмой Dallas Semiconductor. Информация в этом интерфейсе передаётся по единственному проводнику, по нему же получают питание, заряжая внутренний конденсатор в моменты, когда на шине нет обмена данными. Скорость обмена невысокая (максимум 125 Кбит/с), недостаточная для обеспечения передачи данных в момент касания контактного устройства.

Бесконтактные банковские карты используют для передачи данных технологию NFC, разновидность RFID. Платёжные системы, как правило,

используют собственные стандарты, например, Visa payWave, MasterCard PayPass,но устроены они практически одинаково.

Дальность передачи данных через NFC составляет несколько сантиметров. Поэтому первый барьер защиты – физический. Считыватель, по сути, необходимо приложить вплотную к карте, что довольно сложно сделать незаметно.

Зато можно сделать нестандартный ридер, который работает на большей дистанции. Например, исследователи из британского Университета Суррей продемонстрировали возможность считывания по NFC данных на расстоянии до 80 см с помощью компактного сканера.

Такое устройство может незаметно «опрашивать» бесконтактные карты местах массового скопления людей, например в общественном транспорте. Во многих странах они являются некоторым аналогом мелочи в кошельке и имеются практически у всех граждан (например карта Октопус в Гонконге).

Оригинальное решение проблемы расстояния предложили испанские хакеры Рикардо Родригес и Хосе Вилла, представившие доклад на конференции Hack In The Box. Воспользовавшись тем, что современные Android-смартфоны оснащены модулем NFC и нередко «перемещаются в пространстве» физически рядом с бумажником, например, в одной сумке, Родригес и Вилла создали концепт Android-троянца, который превращает смартфон жертвы во что-то вроде ретранслятора NFC-сигнала.

Как только заражённый телефон оказывается возле бесконтактной карты, он отправляет через Интернет злоумышленникам сигнал о доступности транзакции. Мошенники активируют обычный платёжный терминал, подносят к нему свой NFC-смартфон. Таким образом создаётся «мост» через Интернет между NFC-карточкой и NFC-терминалом, удалёнными друг от друга на любое расстояние.

Троянец может распространяться стандартным способом, например в комплекте со взломанным платным приложением. Всё, что требуется, – это версия Android 4.4 и выше. Root-доступ необязателен, хотя и желателен для того, чтобы троянец мог работать и после блокировки экрана.

Демонстрация хакерского взлома бесконтактной чиповой карты экспертом Адамом Лори (Adam Laurie) на конференции Black Hat 2008, дала почву для новых опасений в связи с безопасностью радиочастотной технологии идентификации (RFID), используемой для бесконтактных платежей. Лори использовал для взлома новый скрипт (EMV Chip And PIN credit card reading script), названный ChAP.py. С его помощью удалось считать имя владельца карты RFID-карты American Express, дату окончания её действия, а также номер счёта. Что удивительно, владелец карты при этом даже не вынимал её из бумажника!

Адам Лори, член совета директоров фирмы по безопасности данных компании The Bunker, размести скрипт ChAP.py, написанный на языке Python, в своей онлайн-библиотеке RFIDIOt. Любой может загрузить про-

грамму бесплатно. Сайт также продаёт аппаратные средства, позволяющие считывать и делать запись на RFID-устройства.

Надо сказать, что это не первые проблемы, связанные с безопасностью RFID. В 2006 группа, называющая себя Консорциум RFID по Безопасности и Секретности сообщила, что раскрыла ошибки в защите нескольких типов карт оплаты RFID.

Исследователи проверили приблизительно 20 бесконтактных кредитных карточек и выяснили, что карты RFID передают имена владельца кредитки. Таким образом любое устройство, способное считать информацию, может получить информацию о владельце без его согласия.

Более того, кредитные карты с технологией RFID уязвимы для копирования. Злоумышленник, имея считыватель RFID, может получить информацию с карты, создать её клон, выполнить с помощью полученной копии платежи. Как вариант – мошенник может использовать полученные данные для оплаты покупок в Интернете.

Есть способы, которые помогают снизить риски хищения средств с бесконтактных карт:

– максимальная сумма, которая может быть списана с карты без необходимости ввести пин-код – 1000 рублей, однако есть возможность написать заявление в банк, чтобы её уменьшить; это позволит лишиться меньшей суммы денег в случае, если вор все-таки смог украсть данные вашей карты;

– рекомендуется обязательно подключить SMS-информирование о любых операциях, которые произведены с карты; это позволит вовремя обнаружить кражу и заблокировать карту; несмотря на то, что установлен лимит в 1000 рублей на проведение операции с бесконтактной карты, мошенник может совершить несколько оплат; подключив SMS-информирование, возможно узнать о краже средств уже после первой операции и не позволить списать все деньги с карты;

– быть осторожным и внимательным в местах скопления людей.

Список литературы

1. Бесконтактная банковская карта: принцип работы и безопасность платежей [Электронный ресурс] / – http://visa-mastercard.ru/beskontaktnaya-bankovskaya-karta-princip-raboty-i-bezopasnost-platezhej/

2. Внимание! Владельцам «бесконтактных» банковских карт грозит опасность [Электронный ресурс] / – http://antiko22.info/vse_novosti/vnimanie_vladel_cam_beskontaktnyh_bankovskih_kart_grozit_opasnost/

3. Бесконтактные смарт-карты [Электронный ресурс] / – http://www.russika.ru/ef.php?s=4683

4. Деньги из воздуха: безопасны ли бесконтактные платежи?[Электронныйресурс] / – https://blog.kaspersky.ru/contactless-payments-security/8608/

5. Хакерский взлом бесконтактной чиповой карты [Электронный ресурс] / – https://forum.antichat.ru/threads/63244/

6. БаклагаТ. Как воруют деньги с бесконтактной карты оплаты [Электронный

ресурс] / – http://loxotrona.net/kak-voruyut-den-gi-s-beskontaktnoj-karty-oplaty-visa-paywave-i-mastercard-paypass-pod-pritselom-moshennikov/

УДК 004.057.4, 004.056.5

Пафнутьева Арина Евгеньевна,
студентка 4-го курса, МГУ им. адм. Г.И. Невельского,
Щербинина Инна Александровна,
к. пед. н., МГУ им. адм. Г.И. Невельского, shcherbinina@msun.ru

РЕЙТИНГ ПРОФЕССОРСКО-ПРЕПОДАВАТЕЛЬСКОГО СОСТАВА КАК ИНСТРУМЕНТ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ РАБОТЫ ВУЗА

Вред «уровниловки» в оплате труда отмечался во многих работах, касающихся экономических аспектов управления [1,2]. Объективная оценка эффективности труда по-прежнему остаётся вопросом, который интересует исследователей, поскольку на сегодняшний момент не существует однозначно воспринимаемой методики [3]. Оценка эффективности труда преподавателей затруднена ещё и «нематериальностью» результатов этого труда.

При этом, систему оценки преподавателей можно рассматривать как математическую модель. Большинство предлагаемых методик рассчитывают итоговое значение как сумму некоторых показателей, умноженных на весовые коэффициенты. По полученному значению выстраивается рейтинг.

Существует мнение, которое поддерживается в данном исследовании, что невозможно создать идеальную объективную модель, учитывающую абсолютно все аспекты профессиональной деятельности субъектов оценки. В каждой конкретной ситуации необходимо понимать, что рейтинг преподавателей будет строится с учётом уклона в одну из областей, в зависимости, какую сторону нужно оценивать. Разумеется, есть возможность рассчитывать рейтинг с равными коэффициентами в каждом из критериев, но в таком случае, опять же невозможно претендовать на объективность, так как невозможно выявить аспекты, которые сильнее или меньше влияют на успешность преподавателя.

Обычно выделяются группы критериев, по которым строится система оценки деятельности преподавателей:

- научная работа;
- методическая работа;
- учебная работа;
- воспитательная работа.

Рассмотрев системы рейтинговой оценки преподавателей различных ВУЗов страны в настоящем исследовании были сделаны следующие выводы.

Основные задачи, которые могут решаться с помощью рейтинговой оценки преподавателей:

– повышение мотивации преподавателей к совершенствованию качества профессиональной деятельности, росту квалификации, профессионализма, продуктивности педагогической и научной работы, развитие творческой инициативы;

– повышение обоснованности принимаемых административных решений особенно в сфере кадровой политики;

– контроля результатов учебно-методической, научно-исследовательской, общественной и воспитательной деятельности преподавателей и кафедр и совершенствование её планирования;

– выявление и поддержка эффективно работающей части коллектива;

– мониторинг выполнения плана работыпо различным направлениям.

Принципы организации рейтинговой оценки:

– принцип открытости – рейтинговые данные являются открытыми для ознакомления всего профессорско-преподавательского состава, результаты рейтинга публикуются не позднее, чем за месяц до подведения итогов рейтинга;

– принцип стабильности – критерии оценивания, весовые коэффициенты значимости критериев и методика расчёта рейтингового балла публикуются до начала отчётного периода (учебный год) и не меняются весь отчётный период;

– принцип оцениваемости – критерии оценивания и допустимые значения критериев должны быть чётко определены, не должны допускать двоякого толкования и должны иметь механизмы подтверждения их подлинности;

– принцип трудоёмкости – весовые коэффициенты критериев оценивания определяются исходя из трудоёмкости выполненных работ;

– принцип сравнимости результатов – при расчёте рейтинговой оценки преподавателей необходимо учитывать межотраслевые профессиональные стандарты и производить расчёт рейтинга внутри одной квалификационной группы (ассистент, старший преподаватель, доцент, профессор, заведующий кафедрой, декан);

– принцип расширяемости – каждому заведующему кафедрой предоставляется премиальный фонд баллов (в зависимости от количества ставок ППС за отчётный период) позволяющий отметить в рейтинге работу по направлениям, неучтённым в рейтинге;

– принцип контролируемости – ответственность за достоверность и своевременность предоставленных сведений несёт преподаватель, ответственность за подтверждения сведений, предоставленных преподавателями, несут назначенные ответственные лица в рамках вида оцениваемой деятельности.

Выводы

Рейтинг преподавателей должен быть открытым, гибким механизмом выделения наиболее активной части трудового коллектива и основанием для объективной оценки труда всех преподавателей. Рейтинг должен контролироваться коллегиально (например, на уровне факультета) и нести в себе соревновательное начало.

Список литература

1. Никифорова А. О соотношении роста производительности и заработной платы // Общество и экономика. 2001. № 7–8. С. 95–111.

2. Оплата труда: производство, социальная сфера, государственная служба: Анализ, проблемы, решения / Н.А. Волгин. М.: Экзамен, 2003. 224 с.

3. Григашкина С.И. Методика оценки эффективности заработной платы – Режим доступа – URL:http://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0ahUKEwieyofEvZfQAhWFWSwKHaB3BSUQFggnMAI&url=http%3A%2F%2Fcyberleninka.ru%2Farticle%2Fn%2Fmetodika-otsenki-effektivnosti-zarabotnoy-platy.pdf&usg=AFQjCNEPNp0CudVcRZscDi-bdLPoOmWo6g&bvm=bv.137904068,d.bGg&cad=rjt

4. Васильева Е.Ю., Граничина О.А., Трапицын С.Ю. Рейтинг преподавателей, факультетов и кафедр в вузе: Методическое пособие

УДК 621.396

Пашкеев Сергей Владимирович,

Заместитель начальника кафедры военного обучения ДВФУ

Пузин Олег Владимирович,

начальник кафедры военного обучения ДВФУ

РАЗВИТИЕ МЕТОДОВ И СРЕДСТВ ДОСТАВКИ ВОДОЛАЗОВ К МЕСТУ ПРОВЕДЕНИЯ РАБОТ

Моря и океаны, реки и озера являются кладовой земных богатств, которая до сих пор используется ограниченно и неэффективно.

Россия обладает огромными территориями шельфа. Однако инфраструктура не позволяет, не только вести активную промышленную деятельности, но и осуществлять разведку и исследование подводного мира, представляющего множество опасностей.

Актуальным является формирование научного задела по технической оснащенности средств и методов освоения океана.

Среди множества задач в гидрокосмосе наибольший интерес представляют технические средства обеспечения водолазов.

Объектом исследования является водолазная техника.

Предметом исследования – средства доставки водолазов к месту проведения работ и возвращение на базу.

В состав технических требований для подводной техники входят:

– автономность;

– автоматическое и ручное управление;

– подводная навигация;

– энерговооруженность;

– приемлемая скорость движения;

– широкий диапазон условий по глубине и скорости движения среды;

– широкий диапазон замутненности среды;

– ограничения на массогабаритные характеристики для аппарата, пассажиров и груза;

– радиус действия до сотен километров;

– удобство не только эксплуатации, но и обслуживания;

– тип мокрого размещения водолазов и сухого для груза;

– возможность постановки с различных носителей: с воздушного или иного судна;

– обеспечение задач в экстремальных ситуациях: гидроакустический маяк, и др.

Известны многочисленные конструкции отечественных и зарубежных буксировщиков, которые выполняют одну только функцию - обеспечивают передвижение водолаза под водой.

Это отечественные буксировщики типа "Протей" и "Протон" ("Протей-1", "Протей-2", "Протей-5М", "Протей-5МУ", "Протон", "Протон-У"), а также буксировщики "Нептун" и "Тунец", разработки Особого конструкторского бюро при Ленинградском кораблестроительном институте (ныне Санкт-Петербургский Государственный морской технический университет) [1,2].

Известен также ряд зарубежных буксировщиков: "Пегас", "Кусто", "Марлин" - Франция ("Military Technology", 1996, vol.20, N 3. p.85-89), R-1 - Хорватия (Gane's Intelligens Revue, October, 1994, p.448-452), "МК-1" - США и др. [1,3,4].

Анализ аналогов, а также задач, условий эксплуатации и требований определил состав оборудования на борту и на обеспечивающих судах или на базе размещения.

В состав гидроакустического комплекса возможно включение следующих подсистем:

– носовой и кормовой гидролокатор;

– шумопеленгатор;
– обнаружитель гидроакустических сигналов;
– гидролокатор бокового обзора;
– эхолот;
– лаг;
– оборудование гидроакустической связи;
– гидроакустический навигатор с малой и большой базой;
– имитатор физических полей;
– обнаружитель разводий;
– измеритель толщины льда и др. препятствий;
– аппаратура контроля шумности;
– аппаратура измерения вертикального распределения скорости распространения звука;
– аппаратура измерения скорости течения в ближней зоне;
– устройства опознавания;
– классификатор объектов и оценка их опасности;
– навигационные подсистемы определения элементов движения обнаруженных объектов;
– аппаратура измерения акустического портрета объекта и устройство звуковидения;
– оптические и осветительные приборы, телевизионные камеры;
– измерители физических полей и др. [1,4,5].

Большинство выпускаемых в мире тяжелых буксировщиков (массой более 60 кг) являются буксировщиками нагрудного типа, поскольку дыхательный аппарат водолаза находится на спине [1-5]. Лишь легкие буксировщики (в том числе отечественный буксировщик "Нептун", массой 36 кг) удерживаются водолазом руками впереди себя. Однако существуют и наспинные буксировщики. Например, известный отечественный буксировщик "Протей-2" являлся наспинным. Он был изготовлен под нагрудный дыхательный аппарат, входивший в состав снаряжения ВСОН-61. Буксировщик "Протей-2" является прототипа для группы изобретений [1-5]. Буксировщик "Протей-2" имеет в качестве источника энергии аккумуляторную батарею, (две секции), а в качестве движительного комплекса используется погруженной электродвигатель с гребным винтом в кольцевой насадке.

По аналогичной схеме построено большинство отечественных и зарубежных буксировщиков [1-5]. На водолазе буксировщик крепится с помощью пахового и двух плечевых упоров и поясного ремня. Масса буксировщика 73 кг. Недостатком буксировщика водолаза "Протей-2" является его одно функциональность. Он обеспечивает только передвижение водолаза под водой. Для обеспечения функций навигации, связи, привода, гидролокации, водолазом используются отдельные навигационные и гидроакустические приборы, крепящиеся на водолазе или удерживаются водо-

лазом в руках. Корме того, водолаз не защищен от удара головой о различные подводные препятствия [1-5].

В настоящее время, в связи со значительным уменьшением габаритов навигационной и гидроакустической аппаратуры, появилась возможность часть приборов поместить в буксировщик и обеспечить им питание от его аккумуляторной батареи.

Это позволяет освободить руки водолаза от буксировки приборов навигации и привода и использовать руки для выполнения других задач. Например, в руках водолаз сможет буксировать либо инструмент для подводных работ, либо поисковую гидроакустическую и телевизионную аппаратуру, либо подводную съемочную аппаратуру. Авторы предлагают унифицировать конструкции приведенных выше функциональных устройств для возможного совместного применения. В зависимости от группы планируемых работ предлагается использовать один из базовых вариантов с дооснащением другими модулями из приведенного выше списка оборудования с учетом необходимого дублирования для надежности, но при заданных условиях и ограничениях.

Таким образом, в работе приведен анализ задач, функций и оборудования для буксировщика водолаза, обеспечивающего подводную навигацию, безопасность плавания и свободу рук водолаза.

Список литературы

1. Трошин и др. От водолаза к ихтионавту. – СПб.: Изд-во СПб МТУ, 2004.
2. Транспортировщик водолазов МПК B63C11/46 патента РФ № 207105621 от 27.08.2008
3. Транспортировщик водолазов МПК B63C11/46 патента SU № 844474 от 07.07. 1981.
4. Транспортировщик водолазов МПК B63C11/46 патента GB № 1083422 от 13.09.1967
5. Транспортировщик водолазов МПК B63C11/46 патента РФ № 2330782 от 10.08.2008

УДК 004.052.2

Перцев Алексей Олегович,
Путилова Софья Евгеньевна,
техник лаборатории кафедры БИТС, МГУ им. адм. Г.И.Невельского
Щербинина Инна Александровна,
к. пед. н., декан ФТФ, МГУ им. адм. Г.И.Невельского, shcherb-inina@msun.ru

СУЩЕСТВУЮЩИЕ ПОДХОДЫ К ЗАЩИТЕ КЛИЕНТСКОЙ ЧАСТИ ВЕБ-ПРИЛОЖЕНИЙ

Безопасность веб-приложений принято делить на 2 составляющие – серверную и клиентскую. Изначально противоборство атакующей и защи-

щающейся сторон было сфокусировано на серверной части веб-приложений.

Постепенно защита серверной части совершенствовалась, а клиентская часть все больше усложнялась. Вплоть до того, что в современных веб приложениях сервер присылает всего одну страницу, которая при необходимости может модифицировать свой контент коренным образом, так что пользователю кажется, что он попал на другую страницу. Так снижается нагрузка на сервер и http-соединение. Однако теперь на клиентской стороне хранится всё больше логики приложения, уникальных идентификаторов, сессий и другой чувствительной информации, что всё больше привлекает внимание атакующего.

Ответственность за безопасность клиентской части веб-приложения лежит на его разработчике и браузере. Причём и тем и другим приходится постоянно идти на уступки и поддерживать legacyрешения в целях обратной совместимости. То есть разработчикам приходится отдельно тратить силы, на то чтобы их сайт хорошо работал в старых версиях браузеров, в том числе с точки зрения безопасности. А браузеры поддерживают устаревшие функции и механизмы появившийся за последние несколько лет. Как следствие – все подходы, применяемые разработчиками сайтов и браузеров, для построения защиты приложения сводятся к добавлению всё новых функций и механизмов, вместо качественного пересмотра архитектуры.

Политики безопасности, на которых построена защита приложения в браузере, разрабатывались ещё в начале 90-х годов, и на сегодняшний день не могут полностью удовлетворить запросы разработчиков при построении безопасного веб-приложения. Для одних приложений они слишком строгие, для других наоборот позволяют слишком много. Поэтому появляются всё новые механизмы, призванные обеспечить должный уровень безопасности, но нередко сами становящиеся причиной угроз, особенно в неумелых руках.

Защита клиентской части так же осложняется тем, что, по факту, атакующий имеет возможность исследовать приложение методом белого ящика, поскольку ему доступен исходный код приложения, для получения которого атакующему необходимо сделать один или несколько легитимных запросов. Это усложняет обнаружение атаки и своевременное реагирование на неё со стороны защищающихся.

Одним из подходов обеспечения безопасности веб-браузером является изоляция документа на основе его источника. Это означает, что две веб страницы из разных источников не должны вмешиваться друг в друга, например посредством javaScript. В действительности всё может быть сложнее, поскольку либо нет чётких понятий, где одна страница начинается и заканчивается, либо необходимо более широкое определение источника. Как результат, существует множество поправок и дополнений, которые недостаточно хорошо работают вместе, но не могут быть переделаны

без глубокого вмешательства в уже существующие программные решения и стандарты.

Политика одинакового источника (SOP)это концепт представленный организацией Netscapев 1995 году наряду с языком JavaScriptи объектной моделью документа [0].

Объектная модель документа (DOM) – это не зависящий от платформы и языка программный интерфейс, позволяющий программам и скриптам получить доступ к содержимому HTML-, XHTML- и XML-документов, а также изменять содержимое, структуру и оформление таких документов. [2]

Базовое правило, стоящее заSOP политикой, – любой сценарий JavaScriptдолжен иметь доступ к DOMдругого документа, только если совпадают протокол, доменное имя и порт их источника (табл. 1). Все другие попытки взаимодействия должны пресекаться.

Таблица 1

Примеры политик одинакового источника

Оригинальный документ	**Запрашиваемый документ**	**Internet Explorer**	**Все остальные популярные браузеры**
http://example.com/a/	http://example.com/b/	Доступен	Доступен
http://example.com/a/	http://www.example.com/	Не совпадение домена	Не совпадение домена
http://example.com/	https://example.com/	Не совпадение протокола	Не совпадение протокола
http://example.com:91	http://example.com/	Доступен	Не совпадение порта

В роли протокола обычно выступает HTTP(S), режеFTP и другие. Так как эти протоколы работают поверх протокола TCP, то указывается именно тот, на котором веб-сервер открыл сокет.

SOPреализована во всех современных браузерах с хорошей степенью согласованности, например, Chrome, Firefox. Только InternetExplorer, а так же унаследовавший от него MicrosoftEdge,отличаются от них двумя вещами. Первая это доверенные зоны (trustzones), в которых ограничения SOP снимаются. И вторая, IE исключает порт из определения источника. Это накладывает риски взаимодействия вредоносного JavaScriptкода с не HTTPсервисами и интерпретацией их ответов браузером.

Например, браузер отправляет следующий запрос на порт 25 (SMTP):

```
GET /<html><body><h1>Hi!HTTP/1.1
Host: example.com:25
```

SMTP-сервер интерпретирует его строки как команды и посылает следующий HTTP ответ:

```
220 example.com ESMTP
500 5.5.1 Invalid command: "GET /<html><body><h1>Hi!
HTTP/1.1"
500 5.1.1 Invalid command: "Host: example.com:25"
421 4.4.1 Timeout
```

Все браузеры, следующие рекомендациям RFC,вынуждены обработать этот запрос как тело допустимого HTTP/0.9 ответа и интерпретировать эту последовательность строк как HTMLдокумент, хоть он и не содержит никакой структуры.

Зачастую SOP не обладает необходимой гибкостью, что заставляет разработчиков искать пути её обхода, что естественно подвергает их риску. При необходимости изолировать странички пользователей в социальной сети политика слишком мягкая, так как страницы находятся по разным путям на сервере, а путь не входит в определение источника - где имеет значение лишь протокол, порт и домен. А при кооперации сайтов одной компании, имеющий разные домены 3 уровня (login.example.com ishop.example.com) она слишком строгая.

Рассмотрим некоторые варианты обхода SOP, которые используют разработчики.

1. Использование свойства окна браузера document.domain

С появлением тегов iframeи framestало возможно встраивать несколько документов (страниц) в одно окно браузера и чтобы наладить взаимодействие фреймов, которые делят общий домен верхнего уровня.Для этого можно использовать свойствоJavaScriptdocument.domain.

Например, оба документа, login.example.com., shop.example.com устанавливают свойство окна браузера document.domain равное «example.com». Установка этого свойства перезаписывает обычную проверку по доменному имени, но проверка порта и протокола при этом не меняется. Причём оба документа могут взаимодействовать друг с другом, но не с коренным доменом example.com Чтобы это стало возможным, example.comтоже должен установить свойство document.domain равным «example.com». Это сделано для зашиты от XSSатак с поддоменов. Другой момент – изменение свойства document.domain от его первоначального значения возможно только в сторону домена-родителя.

Здесь часто не учитывается, что теперь всё остальное множество сайтов таких как, например, attacker.example.comтак же становятся «из того же источника», если установят это свойство равное example.com.

2. Использование механизма JSONP

Протокол JSONPпредназначен для кроссдоменного взаимодействия без изменения самого источника. Принцип работы такой – средствами javaScript создаётся тег <script> с атрибутом src, указывающим на необходимый сторонний домен, далее этот тег добавляется в документ, при этом браузер запустит процесс загрузки контента. Чтобы получать ответы со стороннего домена, атрибут scrформируется следующим образом:

```
<scriptsrc="/user?id=123&callback=onUserData"></script>
```

То есть в ответ сервер пришлёт вызов функции onUserDatac необходимыми данными:

```
onUserData({
name: "Леша",
age: 23
});
```

Таким образом, можно запрашивать данные с любого сервера, в любом браузере, без каких-либо разрешений и дополнительных проверок.

Риск безопасности в данном подходе заключается в том, что клиентская сторона полностью доверяет серверной. В ответ может вернуться вызов любой javasciptфункции. НаэтомпостроенаатакаSOME (SameOriginPolicyExecution) илидругое еёназваниереverseclickjacking – если у атакующего есть возможность контролировать атрибут src из-за недостаточной валидации пользовательских данных попадающих на страницу, то он получает неограниченный доступ к выполнению javascriptна странице.

3. Использование функции postMessage

Функция postMessage(), появившаяся в API современных браузеров благодаря стандарту HTML5предоставляетболее строгий механизм взаимодействия сайтов из разных источников, чем описанные ранее. Так как механизм позволяет заранее определить отправителей и получателей сообщений. Это менее удобное, но, при корректной реализации, значительно более безопасное взаимодействие, позволяющее взаимодействовать, в том числе, разным окнам браузера.

К сожалению, разработчики довольно часто совершают ошибки как при реализации логики проверки источника из которого поступило сообщение, так и допуская слишком широкий круг получателей сообщений.

Опаснее всего, когда подобные уязвимости присутствуют в сторонних библиотеках или виджетах, которые используются миллионами других сайтов. В декабре 2016 года Матиас Карлссон (Mathias Karlsson) опубликовал отчёт о найденной уязвимости в популярном виджете AddThis. Виджет представляет собой кнопку на странице, позволяющую поделиться

ссылкой на понравившийся контент с другими пользователями социальных сетей.

При получении сообщения, средствами вызова функции postMessage(), виджет отправлял его на домен s7.addthis.com. Реализовано это следующим образом – создаётся тег <script>и как параметр scrуказывается следующая строка:

```
scriptTag.src = protocol + "//s7.addthis.com/" + messageData;
```

Однако при условии, что messageData уже содержит символы «//» в начале, атрибут определяется по другому:

```
scriptTag.src = messageData;
```

По всей видимости, сделано это было в целях обратной совместимости и перед тем как присвоить значение атрибуту, оно никак не проверялось.

Эта уязвимость позволяла выполнять произвольный кроссдоменный javaScript код в контексте любого сайта имеющего этот виджет. Другими словами была возможность проведения атаки DOMXSS:

```
// Жертва переходит на сайт злоумышленника со встроенным фреймом
// уязвимого сайта
// Так же уязвимый сайт может быть просто открыт в другом окне

<iframe id="frame" src="https://targetpage/using_addthis"></iframe>

// Формируется специальное сообщение содержащее с указанием домена
 // атакующего и вредоносного скрипта, который будет исполнен

<script>
document.getElementById("frame")
.postMessage('at-share-bookmarklet://ATTACKERDOMAIN/xss.js', '*');
</script>
```

Никакого взаимодействия от пользователя не требовалось, жертва должна была только посетить сайт атакующего. На данный момент уязвимость исправлена.

4. Использование политики CORS

Cross-origin resource sharing (CORS) – технология современных браузеров, которая позволяет предоставить веб-странице доступ к ресурсам другого домена. Устроена она следующим образом – если пользовательский javascript совершает попытку кроссдоменного запроса по средством XHR, то браузеры, поддерживающие CORSполитику, подставляют в этот запрос специальный заголовок Origin с указанием текущего домена. Далее сервер обрабатывает значение этого заголовка и в случае, если такой до-

мен присутствует в списке разрешённых разработчиком, то подставляет в ответ заголовок Access-Control-Allow-Origin со значением, равным тому, что отправил браузер. Получив такой ответ, браузер сравнивает заголовки и, если они равны, то передаёт полученный контент javascript обьекту, инициализировавшему соединение.

Браузер может получить от сервера значение «*» в заголовке Access-Control-Allow-Origin, оно указывает браузеру, что на этот сервер обращения разрешены с любых доменов, в том числе и с текущего домена. Это является риском безопасности для такого сервера, кроме случаев когда это действительно необходимо (например, если сервер имеет публичное API).

В случае XSSатаки этот механизм не просто ослабляет SOPполитику, он полностью убирает её ограничения. Так как сервер атакующего может легко вернуть необходимые заголовки в ответе.

5. Использование подхода sever-sideproxy

В данном подходе javascript совершает запрос к своему оригинальному источнику с указанием на какой внешний url он хочет обратиться, а сервер забирает контент с указанного url и отдаёт его клиентской стороне. Способ связан с временными задержками и дополнительной нагрузкой на сервер. В следствии чего, практически не используется.

Таким образом, обеспечение безопасности веб-браузером с помощью изоляции документа на основе его источника требует внимания и особой тщательности в программировании клиентской части веб-приложений, поскольку сам механизм содержит в себе средства обхода ограничений этого механизма.

Список литературы

1. https://en.wikipedia.org/wiki/Same-origin_policy
2. https://ru.wikipedia.org/wiki/Document_Object_Model
3. https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site-00
4. http://resources.infosecinstitute.com/cookies-secure-flag-undesired-behavior-modern-browsers/

УДК 629.12.523

Пляшешник Ксения Николаевна,
преподаватель, Морской колледж МГУ им. адм. Г.И. Невельского

ОСОБЕННОСТИ ДИНАМИКИ МОРСКОГО СУДНА

Мореходными качествами должны обладать как гражданские суда, так и военные корабли. Изучением этих качеств, с применением математического анализа, занимается специальная дисциплина – теория судна. Мореходные качества судна в предмете «Теория судна» изучаются в двух разделах: статике и динамике судна. Статика изучает законы равновесия пла-

вающего судна и связанные с этим качества: плавучесть, остойчивость и непотопляемость. Динамика изучает судно в движении и рассматривает такие его качества, как управляемость, качку и ходкость.

Качкой [2] называется сложное колебательное движение, которое судно может совершать как твердое тело при плавании на спокойной или взволнованной поверхности воды. Возможность колебательного процесса определяется наличием сил или моментов, оказывающих сопротивление перемещениям и стремящихся возвратить судно в исходное положение.

Под действием возмущающей силы судно может иметь шесть возможных видов перемещений: три поступательных в направлении осей x, y, z и три колебательных вокруг этих осей. Однако только три из них могут иметь колебательный характер. Вертикальные колебания (сила действует в направлении оси z), приводящие к периодическим погружениям и всплытиям, называют вертикальной качкой. Колебания вокруг оси y, вызывающие наклонения с борта на борт, называют бортовой качкой (переменный крен). Колебания вокруг оси x, вызывающие продольные наклонения, называют килевой качкой (переменный дифферент).

Сила в направлении оси x вызывает ускорение или торможение движения, а сила в направлении оси y – боковое смещение (дрейф). Момент вокруг оси z вызывает лишь отклонение от курса.

Характеристиками колебательного процесса являются:

1) амплитуда качки – наибольшее отклонение судна от положения равновесия;

2) размах качки – полное перемещение от одного крайнего положения до другого (сумма двух амплитуд следующих друг за другой колебаний);

3) частота качки ω – число полных колебаний судна за время $2\pi t$;

4) период качки t – интервал времени между двумя последовательными колебаниями отклонений судна в одном и том же направлении (два размаха), $t = 2\pi/\omega$;

5) коэффициент динамической качки – отношение амплитуды качки к амплитуде волны, отражающее реакцию судна на воздействие регулярных волн.

Для успокоения наиболее неблагоприятной и опасной бортовой качки применяют специальные меры, заключающиеся в установке успокоителей качки, которые делятся на пассивные и активные. Действие первых основано на использовании энергии качания самого судна, действие вторых – на использовании внешних источников энергии, они искусственно управляются. Рассмотрим наиболее простые и эффективные успокоители качки.

Ходкость – способность судна развивать с помощью движителей заданную скорость, преодолевая сопротивление окружающей среды – воды и воздуха. Сила сопротивления движению судна зависит от физических

свойств среды. Важнейшим физическими характеристиками жидкости являются плотность и вязкость. [1]

Плотностью называется величина, определяемая отношением массы вещества к занимаемому им объему. [1]

Вязкость (внутренне трение) – свойства жидкостей оказывать сопротивление перемещению одной их части относительно другой. [1]

Вязкость жидкости, а также шероховатость поверхности вызывают изменение скорости обтекания вблизи поверхности корпуса. Благодаря молекулярным силам сцепления частицы воды, непосредственно соприкасающиеся с обшивкой корпуса, как бы прилипают к ней и движутся со скоростью, равной скорости судна. По мере удаления от поверхности корпуса скорость частиц в слое воды уменьшается. На некотором удалении частицы имеют скорость невозмущенного потока. Зона, в которой наблюдается изменение скоростей движения частиц жидкости, называется пограничным слоем.

Относительное смещение слоев воды в пограничном слое и изменение при этом гидродинамического давления вдоль смоченной поверхности корпуса вызывают сопротивление движению судна. [1]

Полное сопротивление движению судна складывается из пяти основных составляющих: $R = R_Т + R_ф + R_в + R_{вч} + R_{возд.}$

Сопротивление трения $R_Т$ – равнодействующая сил трения, возникающих вследствие вязкости воды между корпусом движущегося судна и ближайшими к нему слоями воды пограничного слоя. Сопротивление трения зависит от скорости судна, размеров и формы смоченной поверхности корпуса и степени ее шероховатости.

Сопротивление формы $R_ф$ образуется при понижении давления воды за кормой судна и появлении добавочных сил, препятствующих его движению. Равнодействующая сил, возникающих вследствие разности гидродинамических давлений вдоль корпуса и зависящих от его формы, называется сопротивлением формы.

Волновое сопротивление $R_в$ обусловлено влиянием волн на распределение гидродинамических давлений вдоль смоченной поверхности судна.

Сопротивление выступающих частей $R_{вч}$ образуется сопротивлением рулей, насадок, кронштейнов гребного вала и других выступающих частей корпуса. Конструкторы стремятся уменьшить сопротивление выступающих частей, придавая им хорошо обтекаемую форму, и сокращая их число.

Сопротивление воздуха $R_{возд.}$ характеризует воздействие на судно воздушной среды. При проектировании судна для уменьшения сопротивления воздуха надстройкам придают обтекаемую форму и максимально уменьшают их размеры.

Управляемость – мореходное качество, характеризующее способность судна двигаться по выбранной судоводителем или заданной траектории. Управляемость оценивается поворотливостью и устойчивостью судна

на курсе и зависит от гидромеханических свойств судна, эффективности органов управления и действий рулевого. [1]

Поворотливость – способность судна изменять направление движения при перекладке руля или других средств управления. [1]

Устойчивость на курсе – способность судна сохранять заданное направление движения, несмотря на действие течения, волнения и ветра. Эксплуатационную устойчивость судна на курсе проверяют во время ходовых испытаний при ветре 2-3 балла. При этом во время движения заданным курсом регистрируют частоту и углы перекладки руля, необходимые для удержания судна на данном курсе. Если руль приходится перекладывать не чаще 4-6 раз в минуту на углы 2-3°, то эксплуатационная устойчивость на курсе считается достаточной. [1]

Теория управляемости позволяет рассчитать силы, действующие на перо руля и корпус судна при повороте или дрейфе, определить элементы циркуляции, выработать условия устойчивости судна на курсе. Управляемость судна обеспечивается специальными средствами управления, которые создают силу, вызывающую боковое смещение судна.

Средства управления подразделяются на основные и вспомогательные. К основным относятся рули, поворотные насадки, крыльчатые движители, обеспечивающие управляемость судна во время движения, к вспомогательным – подруливающие устройства и активные рули, обеспечивающие управляемость при движении судна по инерции, когда главные двигатели не работают.

Только после всестороннего изучения и проверки на опыте всех мореходных качеств судна приступают к его созданию. Если математическое решение вопроса невозможно, то прибегают к опыту, чтобы найти необходимую зависимость и проверить выводы теории на практике. Построение и анализ моделей динамики судна направлены в первую очередь на выявлении и изучении объективных закономерностей, описывающих взаимодействие корабля с внешней средой, которые в одинаковой мере присущи мореходным качествам всех кораблей независимо от их индивидуальных различий. Знание этих закономерностей дает возможность предвидеть поведение корабля в различных условиях, а также указать те предупредительные меры, которые нужно предпринять, для исключения гибельных последствий, что имеет большое значение, как для кораблестроителей, так и для мореплавателей. С точки зрения постройки судов наличие моделей, обеспечивающих качественные оценки поведения судна под воздействием внешней среды (в том числе и экстремальных ситуаций) в зависимости от его размеров, формы корпуса, распределения грузов и т.п., предоставляет возможность обеспечить кораблю надлежащие мореходные качества еще на этапе проектирования.

В настоящее время можно выделить четыре категории моделей динамики морских объектов: спектральные линейные и линеаризованные модели динамики судна; нелинейные асимптотические модели динамики

судна, нелинейные численные модели динамики судна, основанные на уравнениях классической механики; нелинейные численные модели динамики судна, основанные на уравнениях гидромеханики.

Данные модели имею разное назначение, и могут использоваться для различных классов задач и условий их применения. Однако численные методы построения моделей могут привести к потере новых решений. Поэтому целесообразно разработать более точные методы построения моделей, позволяющих решать широкий класс задач, связанный с динамикой судов на волнении, в некоторых случаях позволяя получать результаты, сопоставимые по точности с экспериментами в опытовых бассейнах.

Список литературы

1. Басин А.М. Ходкость и управляемость судов. М.: Транспорт, 1977. - 456с.
2. Смирнов Н.Г. Теория и устройство судна. – М.: Транспорт, 1992. – 248с.

УДК 534.014.4, 537.862

Попов Игорь Павлович
научный консультант, Центр высоких технологий, г. Курган,
e-mail: cht.045@mail.ru

СПОНТАННЫЕ УПРУГО-ЕМКОСТНЫЕ КОЛЕБАНИЯ В СИСТЕМАХ АВТОМАТИКИ

Введение

В составе систем автоматики используются, в частности, линейные электромеханические преобразователи с пружинными возвратными механизмами.

Пружина обладает способностью, как запасать, так и отдавать потенциальную энергию. Если при этом не происходит потерь энергии, то логично предположить, что указанное свойство пружины должно обусловливать наличие некоего реактивного сопротивления преобразователя, которое также характеризуется обменом энергии без ее диссипации.

Актуальной задачей является выявление влияния упругости пружинного механизма преобразователя на реактивное сопротивление его электрической цепи и вытекающей из этого возможности возникновения свободных гармонических колебаний, которые могут иметь отрицательное воздействие на систему. Предпосылкой решения этой задачи является одна из двух систем аналогий между электромагнитными и механическими величинами, в соответствии с которыми упругость связана дуальным соотношением с индуктивностью

$$\frac{1}{k} \Rightarrow L .$$

Однако дуальная связь не является функциональной, поскольку охватываемые ею величины относятся к изолированным друг от друга системам. Поэтому указанное соотношение само по себе не дает оснований рассматривать механическую величину коэффициент упругости в качестве параметра электрических цепей.

Целью настоящей работы является представление упругой нагрузки в виде индуктивного сопротивления линейного электромеханического преобразователя и обоснование возможности возникновения свободных гармонических колебаний при подключении к нему конденсатора, играющего роль эквивалентного емкостного сопротивления электрической цепи преобразователя.

Упруго-емкостная система

Упрощенная модель системы представлена на рисунке. Коэффициент упругости пружины k, магнитная индукция в зазоре B, между полюсами находятся n проводников с длиной активной части l [1–2]. Емкость конденсатора C. Активное сопротивление, потери на трение, индуктивность, емкость и масса обмотки не учитываются.

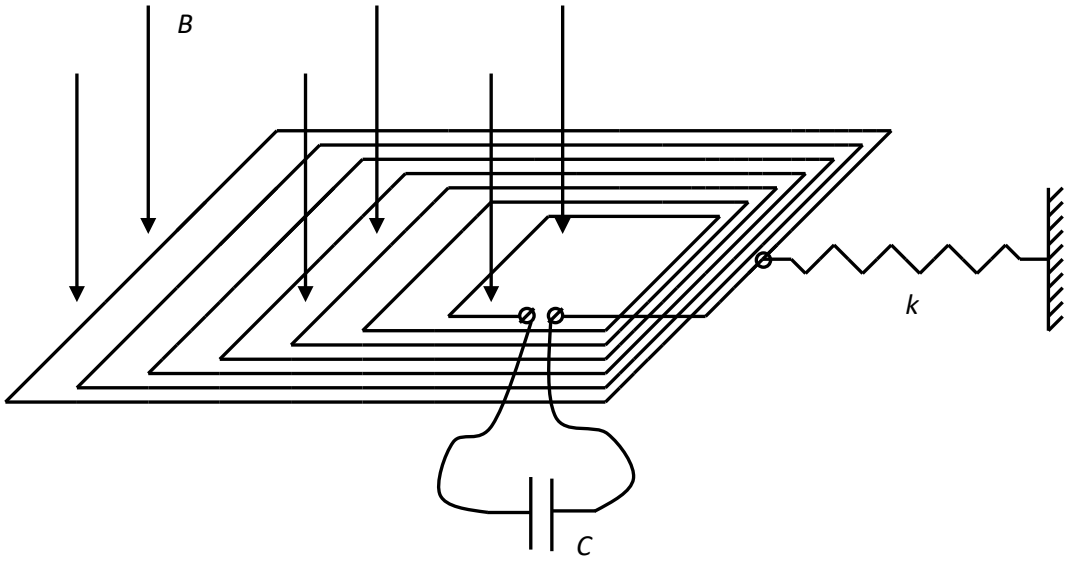

Рис. 1. Упруго-емкостная (kC) колебательная система

Возникновение свободных гармонических колебаний

Механическое и электрическое состояния kC колебательной системы описываются двумя уравнениями в соответствии с законами Гука, Ампера и вторым законом Кирхгофа:

$$kx = Blni\,, \tag{1}$$

$$Bln\frac{dx}{dt} + u_C(0) + \frac{1}{C}\int_0^t idt = 0\,. \tag{2}$$

Здесь x – перемещение обмотки, $Blni$ – сила Ампера, $Blndx/dt$ – ЭДС электромагнитной индукции. Последнее слагаемое – напряжение на конденсаторе.

$B, l, n,$ – параметры, обусловливающие электромеханическое взаимодействие. Их целесообразно объединить в параметрический коэффициент

$$y = \left(Bln\right)^2. \qquad (3)$$

Пусть начальные условия:

$$u_C(0) = u_0,\ i(0) = 0.$$

Производная (1) с учетом (3) имеет вид:

$$\frac{dx}{dt} = \frac{y^{0,5}}{k}\frac{di}{dt}.$$

При подстановке в (2) получается выражение:

$$\frac{y}{k}\frac{di}{dt} + u_C(0) + \frac{1}{C}\int_0^t idt = 0.$$

Дифференцирование последнего соотношения дает классическое дифференциальное уравнение свободных гармонических колебаний [3–4]:

$$\frac{d^2i}{dt^2} + \frac{k}{yC}i = 0.$$

Его решение:

$$i = I_m \sin\omega_0 t,$$

$$I_m = u_0\sqrt{\frac{kC}{y}} = \frac{u_0}{X_{kC}}.$$

$$X_{kC} = \sqrt{\frac{y}{kC}}$$

– волновое сопротивление,

$$\omega_0 = \sqrt{\frac{k}{yC}} \qquad (4)$$

– собственная частота автономной консервативной kC-системы.

Таким образом, в рассматриваемой kC колебательной системе могут возникать свободные гармонические колебания.

Заключение

Свободные гармонические колебания могут происходить при взаимодействии величин различной физической природы – упругости и электрической емкости.

В традиционных колебательных системах происходит взаимное превращение энергии, обусловленной движением, – кинетической энергии и энергии магнитного поля в энергию, обусловленную положением, – энергию деформированной пружины и энергию электрического поля. В отли-

чие от них в kC-системе происходит взаимное превращение энергии, обусловленной положением, – потенциальной энергии пружины в энергию, также обусловленную положением – в энергию электрического поля конденсатора.

Сопоставление выражения (4) с формулами для собственных частот механического маятника:

$$\omega_0 = \sqrt{\frac{k}{m}}$$

и электрического колебательного контура:

$$\omega_0 = \frac{1}{\sqrt{LC}}$$

позволяет установить существование искусственных механических и электрических величин [5–9].

Искусственная (емкостная) масса:

$$m_C = yC\,.$$

Искусственная (инертная) емкость:

$$C_m = \frac{m}{y}.$$

Искусственная (упругая) индуктивность:

$$L_k = \frac{y}{k}.$$

Искусственная (индуктивная) упругость:

$$k_L = \frac{y}{L}.$$

В соответствии с этими выражениями (4) можно представить в виде:

$$\omega_{0kC} = \sqrt{\frac{k}{yC}} = \frac{1}{\sqrt{CL_k}} = \sqrt{\frac{k}{m_C}}\,,$$

т.е. либо как электрический колебательный контур с искусственной индуктивностью, либо как механический маятник с искусственной массой. При этом в некоторой мере реализуется принцип суперпозиции состояний системы [10].

Полученные выражения устанавливают функциональные зависимости между электрическими и механическими величинами.

Список литературы

1. Попов И.П. Емкостно-инертное устройство // Известия Санкт-Петербургского государственного электротехнического университета «ЛЭТИ». – 2015. – Том 2. – С. 43–45.

2. Попов И.П. Установление частной функциональной зависимости между емкостью и массой // Вестник Курганского государственного университета. Естественные науки. – 2011. – Вып. 4. – №2(21). – С. 85–87.

3. Попов И.П., Сарапулов Ф.Н., Сарапулов С.Ф. Инертно-индуктивный осциллятор // Вестник Курганского государственного университета. Технические науки. – 2013. – Вып. 8. – № 2(29). – С. 80, 81.

4. Попов И.П. Упруго-индуктивный осциллятор // Российский научный журнал. – 2013. – № 1(32). – С. 269, 270.

5. Попов И.П. Реализация частной функциональной зависимости между индуктивностью и массой // Российский научный журнал. – 2012. – № 6(31). – С. 300, 301.

6. Попов И.П. Зависимость реактивного сопротивления пьезоэлектрического преобразователя от механических параметров его нагрузки // Научно-технический вестник информационных технологий, механики и оптики. – 2013. – № 5 (87). – С. 94–98.

7. Попов И.П. Вращательные инертно-емкостные устройства // Вестник Самарского государственного технического университета. Технические науки. – 2011. – №3(31). – С. 191–196.

8. Попов И.П. Искусственные масса и упругость // Вестник Тверского государственного технического университета. – 2016. – № 1(29). – С. 7–11.

9. Попов И.П., Чумаков В.Г., Родионов С.С., Шевцов И.В, Низавитин С.С., Михайлов В.В. Упругая емкость в цепи питания пьезоэлектрического преобразователя // Вестник Курганского государственного университета. Технические науки.– 2016. – Вып. 11. – № 3(42). – С. 87–89.

10. Попов И.П. Суперпозиция состояний как принцип моделирования // Вестник Морского государственного университета им. адмирала Г. И. Невельского. Серия: Автоматическое управление, математическое моделирование и информационные технологии. – 2016. – Вып. 75. – С. 75–81.

УДК 621.37

Стволовая Анастасия Константиновна,
магистрант, ВГУЭС, г. Владивосток
Павликов Сергей Николаевич,
к.т.н., зав. каф. РЭРС, профессор, МГУ им. адм. Г.И. Невельского
Убанкин Евгений Иванович,
к.т.н., доцент кафедры РЭРС, доцент, МГУ им. адм. Г.И. Невельского

МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ В МОБИЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Объект исследования – радиоканал передачи информации. Предмет исследования – скрытность радиоканала. Цель – разработка и исследование методов защиты информации, передаваемой по радиоканалам на основе управления разделением информации по ресурсам доставки элементов сообщения, что позволяет увеличивать энергетическую защищенность сообщений. В мире очень часто сталкиваются с проблемой несанкционированного использования передаваемой информации. Существуют методы, базирующиеся на математических задачах, которые снижают эффективность защиты из-за ограниченного представления сигналов, каналов и методов их трансформации, поэтому необходим поиск других методов. В работе разрабатывается метод, который позволит повысить эффективность защиты информации на базе пространственного разделения и зашумления [1].

Работа данного метода заключается в разделении информации на несколько частей. Подразумевая деление информационных блоков на две составляющие дополняющие друг друга. Первая составляющая – информация, вторая – ключ. Разделение происходит следующим образом: исходный информационный сигнал во времени переводится в спектр, из спектра вычитаются заданные компоненты в виде дискретных составляющих, оставшийся обрезанный сигнал переводится снова во временную область и потом подается к антенне для излучения. После этого вырезанные части ключа также преобразуются из спектра во временную область и подаются на передатчик также, как и ложная информация. В результате получаем три потока: ключ, обрезанная информация и ложная информация. Антенны передатчиков формируют излучение передаваемой информации по направлению к определенной заданной точке. Ключ формируется другой антенной системой и направляется под углом так, чтобы обрезанная информационная составляющая и ключ сложились синфазно в заданной точке пространства. Вокруг полезной передаваемой информации излучается ложная информация. Это происходит с целью создания фона чтобы отвлечь внимание противной стороны. Приемной стороне заранее известно в какой точке необходимо будет осуществлять съем информации в этом направлении и будет сфокусирована приемная антенна. В этой точке уже будут сложены обрезанная информация и ключ, в результате принимающая сторона имеет возможность получить часть нужной информации.

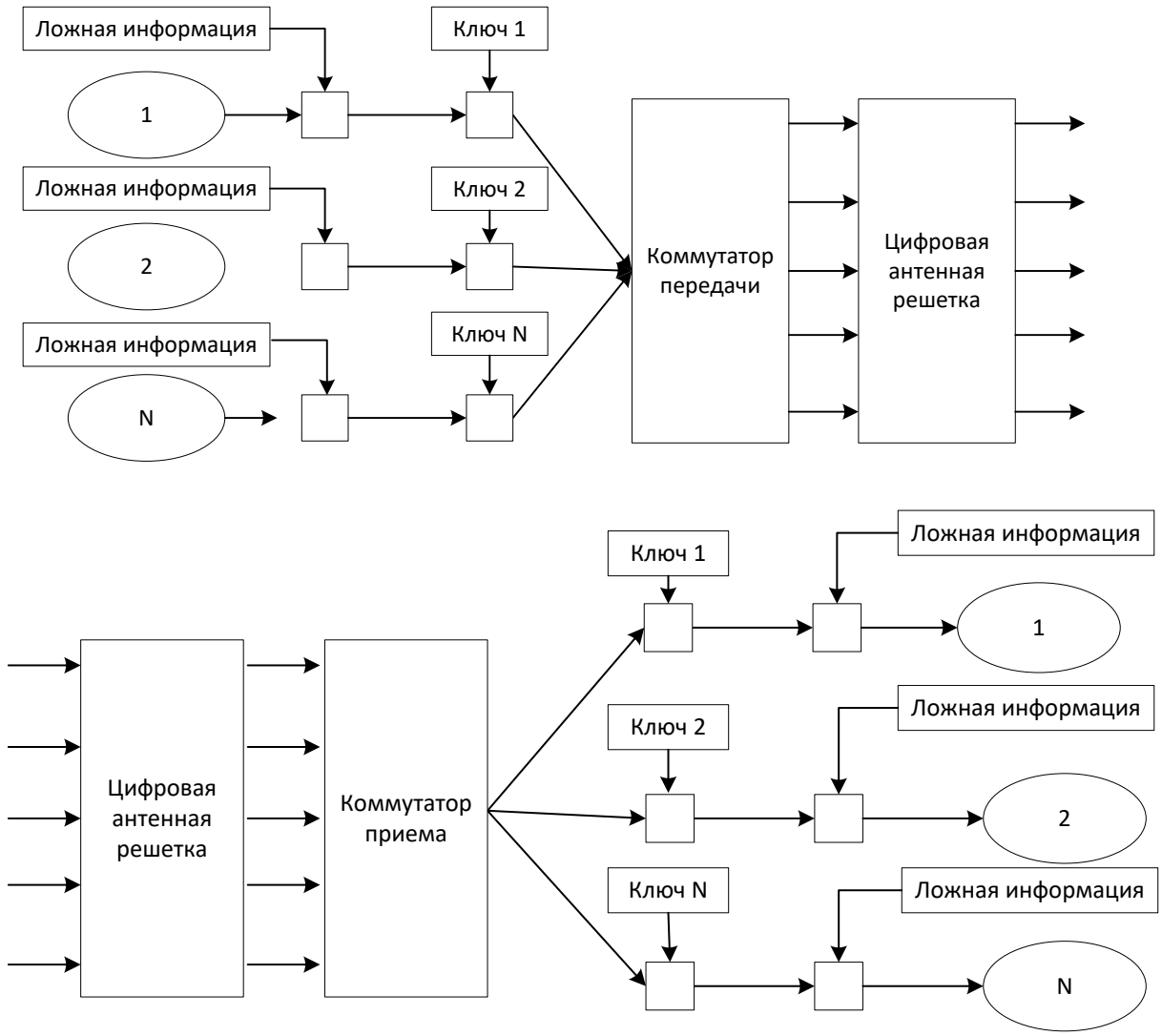

Рис. 1. Принцип работы метода защиты информации

После того как необходимые данные будут приняты в заданный момент времени, система перестроится для приема информации в следующей точке и в другой участок времени. Преимуществом является то, что информационная система имеет ограниченное количество каналов. Если мы увеличиваем количество ложной информации, трасс передачи информации, частот то мы тем самым снижаем скорость передачи и упрощаем процесс по вскрытию механизма закрытия информации противной стороны.

Для реализация метода необходимо выполнение следующих условий: выбранные точки должны быть видны на приемной и передающей стороне одновременно. Приемник и передатчик могут не находиться в зоне прямой видимости, но точка, в которую излучается информация, должна быть видна двум сторонам; область пространства, в которой передается информация, должна определяться сектором в заданных пределах. Противная сторона вынуждена будет просматривать множество точек, но не

зная, как собирается информация во времени и каким образом осуществляется переход с одной точки на другую, возможность вскрытия будет минимальна. Это и может привести к перегрузке информационной системы злоумышленников и прекращению несанкционированного съема [2]. На рисунке 2 приведен пример трассы, по которой передается информация, а также указано возможное положение противной стороны при осуществлении сеанса связи. Техническое решение [2, 3] по реализации метода представлено на рисунке 3.

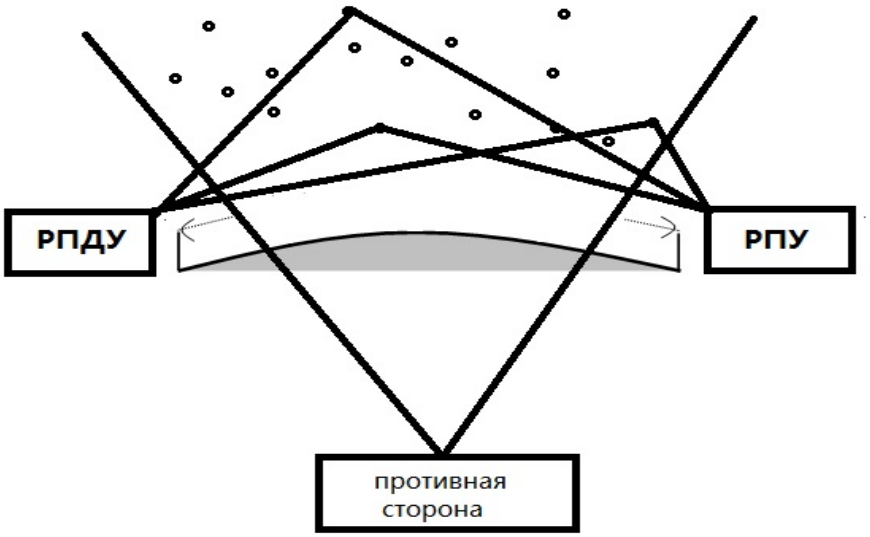

Рис. 2. Графическое изображение сторон в момент сеанса связи

Таким образом, продемонстрировано, что даже наличие высокопроизводительных компьютеров не сможет обеспечить вычисления всех вариантов возможных точек, в которых можно получить информационную составляющую. Поэтому вариантов столько, сколько точек в зоне прямой видимости абонентов. При этом получение информации обуславливается не только выбором точки, но и также зависит от периода жизни этой точки, ключа, частоты, и поляризации.

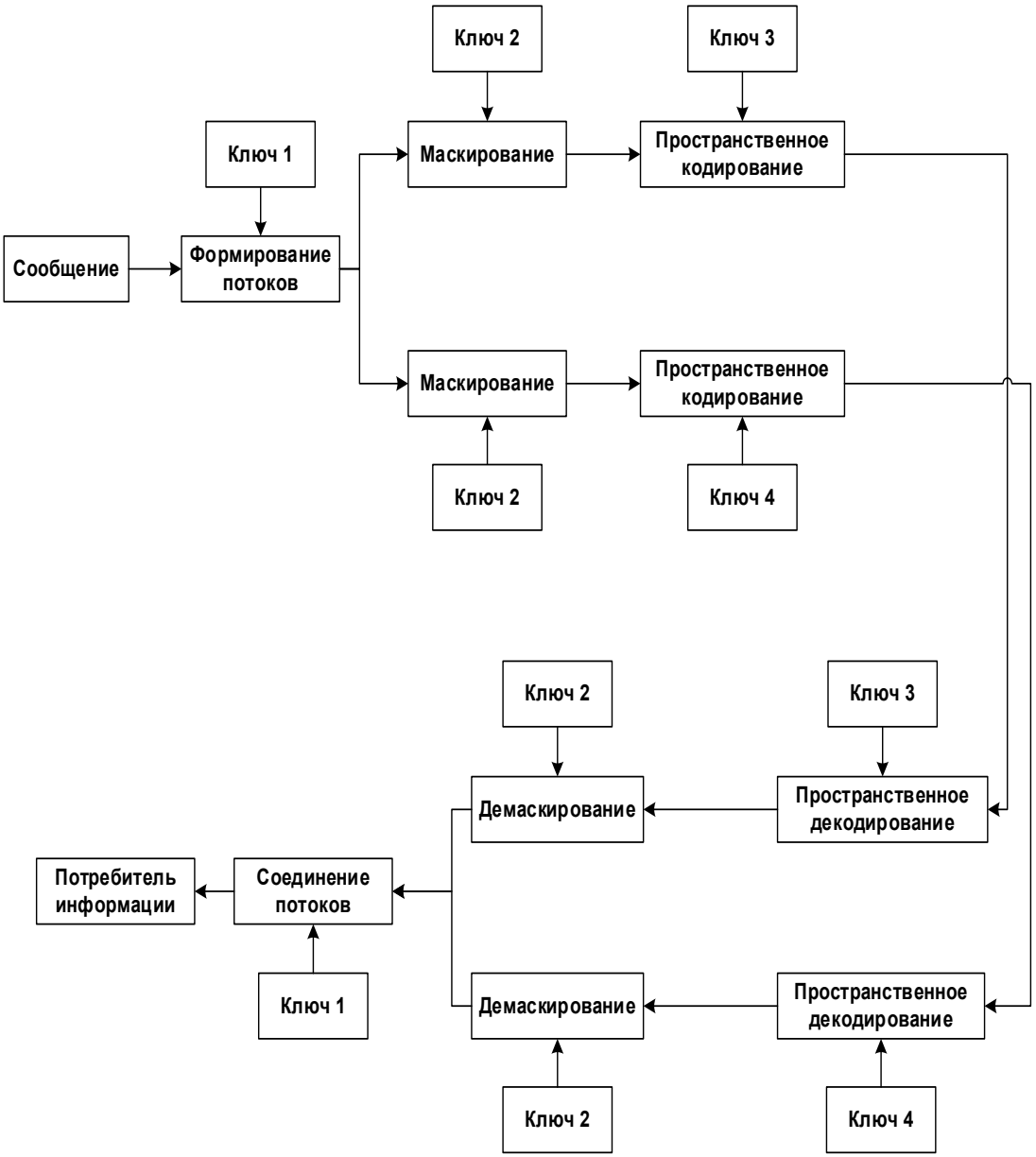

Рис. 3. Техническое решение

К тому же мы можем пойти другим путем, задать на приемной стороне вырезанные дискреты, где уже, в свою очередь, они и будут восстановлены. То есть принятый временной сигнал, который преобразуем в спектр, к этому спектру добавляем спектр ключа, полученные в частотной области составляющие преобразуем во временную и она является информационной составляющей. Предложенный метод найдет применение в системах мобильной связи 5G в которых расширяются функции пространственного кодирования за счет применения цифровых антенных решеток как в мобильном терминале так и на базовой станции. Предложенная технология позволит продлить срок эксплуатации принципа одного арендатора частотного ресурса, но позволит поднять эффективность мобильных систем на совместной территории при кооперативном использовании частотного спектра.

В работе предложен метод защиты информации в радиоканале, значительно затрудняющий работу станциям радиоразведки. Разработка метода пространственного преобразования, позволит повысить скрытность передаваемой информации и увеличить защищенность сообщений

Таким образом, разработка метода пространственного преобразования позволит: повысить скрытность передаваемой информации, увеличить защищенность сообщений.

Список литературы

1. Помехоустойчивость и эффективность систем передачи информации [Текст] / А.Г. Зюко, А.И. Фалько, И.П.Панфилов. Под ред. А.Г. Зюко. – М.: Радио и связь, 1985.

2. Усовершенствование технического решения по модернизации мобильных устройств сотовой связи: сб. докладов 62 международной молодежной научно-технической конференции «Молодежь. Наука. Инновации»; МГУ им. адм. Г.И. Невельского. – Владивосток: Изд-во МГУ им. адм. Г.И. Невельского, 2014. – 221-225с.

3. Техническое решение по модернизации мобильных устройств сотовой связи: сб. докладов 61 международной молодежной научно-технической конференции «Молодежь. Наука. Инновации»; МГУ им. адм. Г.И. Невельского. – Владивосток: Изд-во МГУ им. адм. Г.И. Невельского, 2014. – 222с.

УДК 621.37

Убанкин Евгений Иванович,
к.т.н., доцент кафедры РЭРС, доцент, МГУ им. адм. Г.И. Невельского
Стволовая Анастасия Константиновна,
магистрант, ВГУЭС, г. Владивосток
Павликов Сергей Николаевич,
к.т.н., зав. каф. РЭРС, профессор, МГУ им. адм. Г.И. Невельского

МЕТОД МАСКИРОВАНИЯ ИНФОРМАЦИИ

Объект исследования – широкополосный канал передачи информации.

Предмет исследования – скрытность радиоканала

Цель – повышение защищенности информации за счет использования метода обработки в перспективных системах связи с широкополосными сигналами.

В наше время темпы развития информационных технологий постоянно растут. Существуют методы, базирующиеся на изучении сигнала в узкополосном канале. Передача информации таким способом снижает эффективность защиты из-за ограниченного представления сигналов, поэтому необходимо использование широкополосного канала с использованием фильтра Гильберта.

Рассмотрим общую классификацию маскирования речевых сообщений рисунок 1. Суть предлагаемого метода состоит в формировании про-

странственного режекторного отклика передающей антенны. Речевой сигнал проходит через данный фильтр, после чего передается принимающей стороне. Данный метод предполагает, что противнику будет сложно понять по какой «трассе» передается сигнал.

Рис. 1. Классификация методов маскирования сообщений

Согласно предполагаемому методу будет использоваться режекторный фильтр (рис. 2).

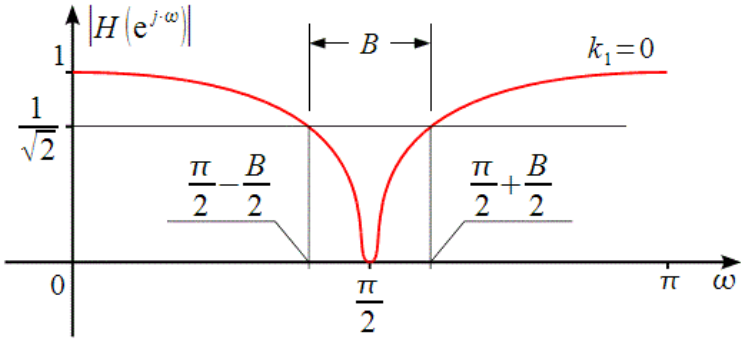

Рис. 2. Режекторный фильтр

Поскольку $k_1 = 0$, то АЧХ симметрична относительно частоты режекции $\omega_0 = 0.5 * \pi$, тогда обозначим полосу фильтра по уровню $1/$

$\sqrt{2}$ как В. Таким образом необходимо найти такое значение k_2 при котором АЧХ режекторного фильтра при $k_1 = 0$ на частоте $\omega = \beta = \frac{\pi}{2} + B/2$ была бы равна $1/\sqrt{2}$, т.е.

$$\left|H(e^{j\beta})\right| = \frac{1}{2} * (1 + k_2) * \sqrt{\frac{2+2*\cos(2*\beta)}{1+k_2^2+2*k_2*\cos(2*\beta)}} = \frac{1}{\sqrt{2}}.$$

Рассмотрим три метода маскирования информации по таблице 1.

Таблица 1

Три метода маскирования информации

Метод	**Особенность**	**Влияние на работу РР/РТР**	**Влияние на приемник**
Пространственный режекторный отклик передающей антенны	Легко запилинговать (энергетически) место РПД	С внедрением затрудняется задача съема информации	Влияние на приемник не сказывается
Съем информации с канала за счет неоднородностей рассеяния	Высока неопределенность трассы	Остается высокая неопределенность	На приемник не отражается
Съем информации в случае где известно нахождение приемника	Приемник не имеет демаскирующих признаков и определение его местоположения затруднено с внедрением нового технического решения. Принимаем информацию в районе приемника.	Задача более усложняется для станции РТР	На приемник не влияет
Съем информации в случае где не известно нахождение приемника		Задача более усложняется для станции РТР	На приемник не влияет

Рассмотри один из методов подробнее. Будем формировать всенаправленную антенну, но в каком-то одном направлении используем вращающуюся часть антенны. Из-за данного вращения не происходит излучение. В одном месте имеется фильтр преобразование Гильберта – противосигнал смещение на π 180 градусов. И только после прохождения через данный фильтр происходит излучение.

Потребители: производители телекоммуникационного оборудования и пользователи систем связи с улучшенными характеристиками. Расширение информационного пространства сигнала, канала и ложных маскирующих данных позволяет говорить о значительном увеличении скрытности канала передачи информации за счет расширения пространства возможных элементов различения ресурсов применяемых для передачи информации по каналу.

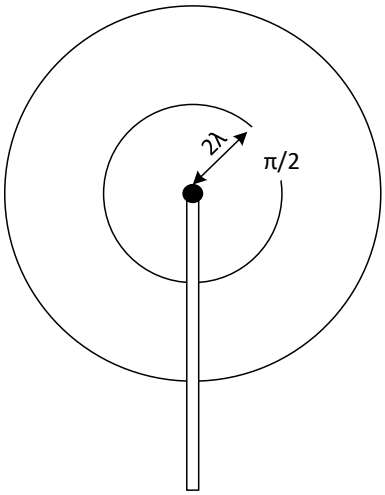

Рис. 3. Излучение ШП преобразование Гильберта

Анализ показывает, что увеличение пространства возможных элементов разрешения ресурсов по которым идет трансляция ложной информации их совместное использование для увеличения информационной нагрузки на станции радиоразведки, радиоэлектронной разведки, а также введение в формуле пропускной способности элементов разрешения, говорит о том, что такое преобразование формулы Шеннона открывает новые возможности по увеличению пропускной способности. За счет уменьшения элементов разрешения используемого ресурса и это затрудняет для радиоразведки процесс съема и перехвата разрешающей способностью элемента, используемого для передачи информации и разрешенный способ станции радиотехнической разведки. В случае если элемент разрешения радиоразведки больше, это приводит к увеличению шумов и ложных сигналов то есть снижение отношения сигнал/помеха. Если же элемент разрешения станции радиоразведки значит меньше, чем элемент разрешения используемой для передачи информации, то это ведет к потере части информации.

Таким образом, в работе предложен метод использования передачи информации в широкополосном канале с помощью преобразования Гильберта, что помогает передавать информацию с высокой защищенностью.

Список литературы

1. Стволовая А.К. Технология квадратурной обработки в системах связи. [Текст]: монография – Владивосток: Мор. Гос. ун-т, 2013. – С. 402 - 405.

2. Построение режекторного фильтра на основе всепропускающего [Электронный ресурс]. - Режим доступа: http://www.dsplib.ru/content/notch/notch.html

УДК 531:681.5.01:629.5

Чинчукова Елена Павловна
ст. преподаватель кафедры теоретической механики и сопротивления материалов, МГУ им. адм. Г.И. Невельского,
Chinchukova_lena@mail.ru
Поршкевич Наталья Юрьевна*,*
доцент кафедры Менеджмента и логистики МГУ им. адм. Г.И. Невельского,
Чижиков Никита Романович*,*
Аспирант ДВФУ, г. Владивосток

ИДЕНТИФИКАЦИЯ ПАРАМЕТРОВ НЕЛИНЕЙНОЙ МОДЕЛИ СУДНА С ИСПОЛЬЗОВАНИЕМ СТЕПЕННЫХ РЯДОВ

Настоящая работа посвящена проблемам идентификации параметров нелинейного объекта, в частности – судна. Эта задача имеет важное значение для построения системы управления судна или других морских подвижных объектов (МПО). Общая модель судна представляет собой набор дифференциальных уравнений высокого порядка, для частных задач, например задач управления курсом судна используется упрощенные модели – линейная модель Номото первого и второго порядка, а так же нелинейные модели Норбина и Беха [8,6,7]. Линейные модели представляют собой существенно упрощенные модели, более адекватными и близкими к реальной модели судна являются нелинейные модели. В настоящей статье решается задача определения параметров нелинейной модели судна. Основная идея заключается в разложении неизвестной функции, описывающей вязкое сопротивление, в степенной ряд и тем самым сведении задачи определения функции к задаче определения коэффициентов, т.е. к параметрической идентификации.

Рассмотрим модель судна, как нелинейную модель Норбина I порядка [6,7,8,9,10] со следующей структурной схемой, рис. 1.

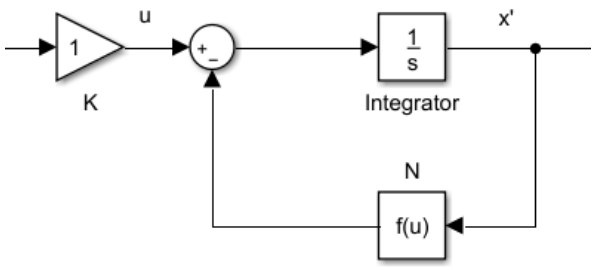

Рис. 1. Структурная схема модели Норбина I-порядка

На рис. 1 функция f(x)-нелинейная функция:

$$f(x) = c_3x^3 + c_2x^2 + c_1x + c_0$$

Математическую модель ОУ можно представить в общем виде:

$$\dot{x} = f(x) + Ku \ , \qquad (1.1)$$

где K – коэффициент управления, u – функция управления, f(x)- нелинейная функция с неизвестными параметрами и структурой, описывающая влияние вязкого сопротивления на курс судна.

Математическая модель эталонной модели описывается следующим уравнением:

$$\dot{x_м} = f_м(x) + K_м u + V \ , \qquad (1.2)$$

где функция $V = \gamma \ sign \ e$ – функция повышающая качество управления.

Так как любую функцию можно разложить в ряд, например Тейлора, представим f(x):

$$f(x) = \sum_1^n a_i x^i \qquad (1.3)$$

Тогда в эталонной модели $f_м(x)$:

$$f_м(x) = \sum_1^n a_{м_i} x^i \qquad (1.4)$$

Для идентификации воспользуемся ***методом скоростного градиента*** [1,2,3]

Согласно этому методу – необходимо воспользоваться целевой функцией Q, пусть:

$$Q = \frac{1}{2} e^2 \ , \qquad (1.5)$$

где $e = x - x_d$ – разница между выходным сигналом объекта и выходным сигналом модели.

Чтобы найти $a_{м_i}$ и $K_м$ определим чему равна производная по времени $\dot{Q}$.

$$\dot{Q} = e\dot{e} = e(\dot{x} - \dot{x_d}) = e(\sum_1^n a_i x^i + Ku - \sum_1^n a_{м_i} x^i - K_м u - V) \qquad (1.6)$$

Исходя из формулы (1.6) найдем:

$$\dot{a_{м_1}} = -ex^i \ , \ \dot{K_м} = -eu \qquad (1.7)$$

Далее приведены результаты идентификации коэффициетов объекта управления при различных значениях коэффициентов эталонной модели (рис. 2).

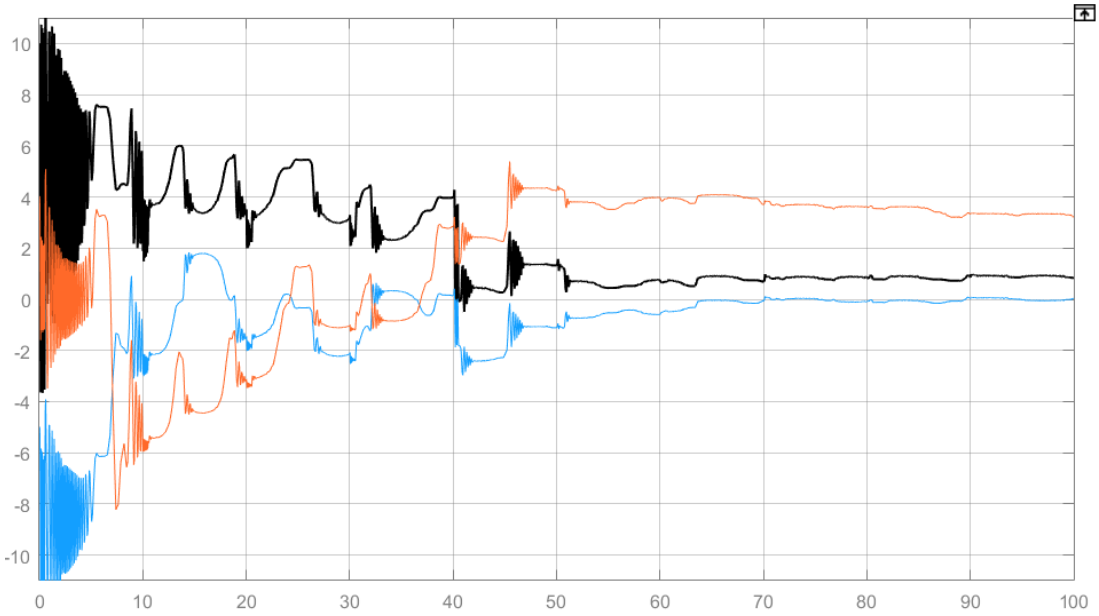

Рис. 2. Графики, показывающие процесс идентификации коэффициентов функции $f_м(x)$, верхний (красный) график - $a_{м_1}$, средний (черный) - $a_{м_3}$, нижний (синий) - $a_{м_2}$

Как видно из графика – все коэффициенты принимают значения коэффициентов объекта управления. При изменении значений коэффициентов a_i, в функции f(x). Значения коэффициентов в настраиваемой модели так же изменятся. Изменив функцию f(x) на $f(x) = 3x^3 + x$, получаем графики настройки коэффициентов, изображенные на рисунках 3-5.

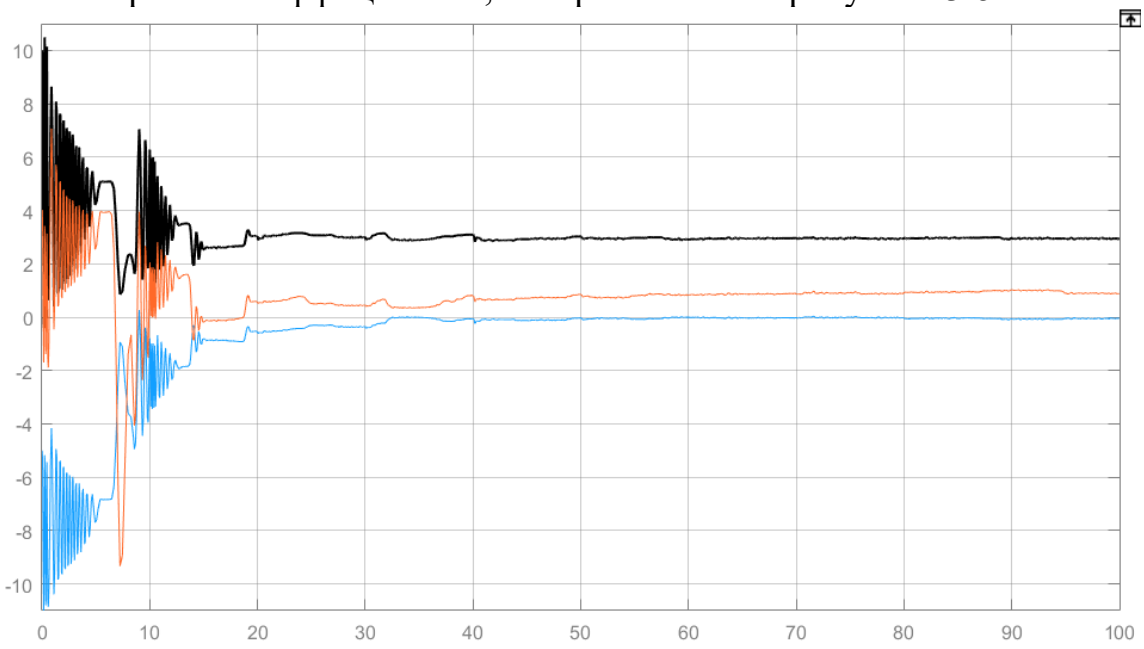

Рис. 3. Графики, показывающие процесс идентификации коэффициентов функции $f_м(x)$, верхний (черный) график - $a_{м_1}$, средний (красный) - $a_{м_3}$, нижний (синий) - $a_{м_2}$

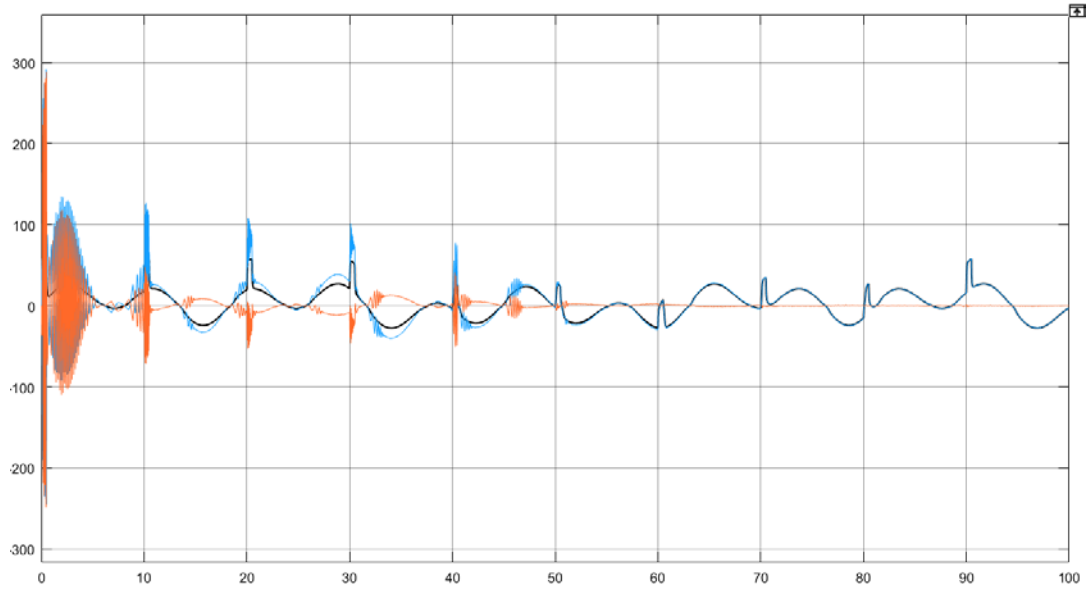

Рис. 4. Графики настройки сигналов модели (x_d) – черный график, объекта (x) – синий график, их разницы (e) (ошибки настройки сигналов) - красный график

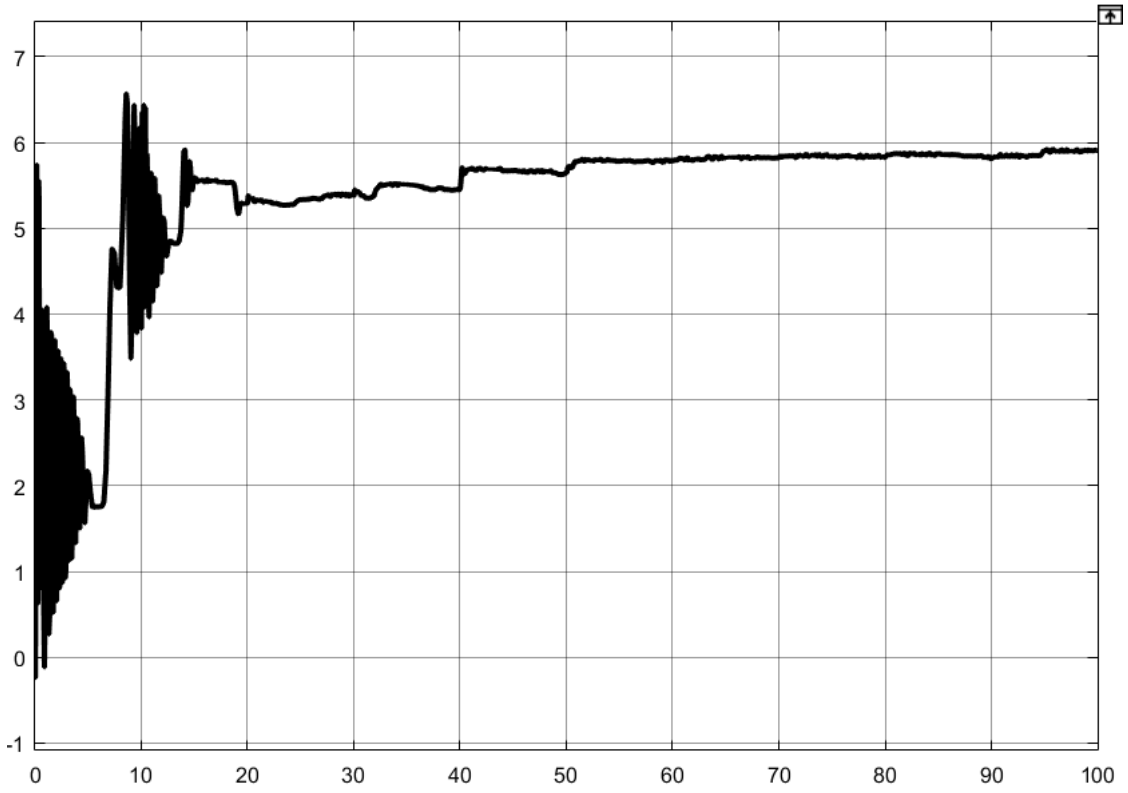

Рис.5. График настройки коэффициента модели $K_м$

Далее покажем графики настройки коэффициентов $a_м$, $K_м$ и сигналов x, x_d и e при различных функциях $f(x)$.

Если $f(x) = 2x^3$, получаем графики настройки коэффициентов, изображенные на рисунках 6-8.

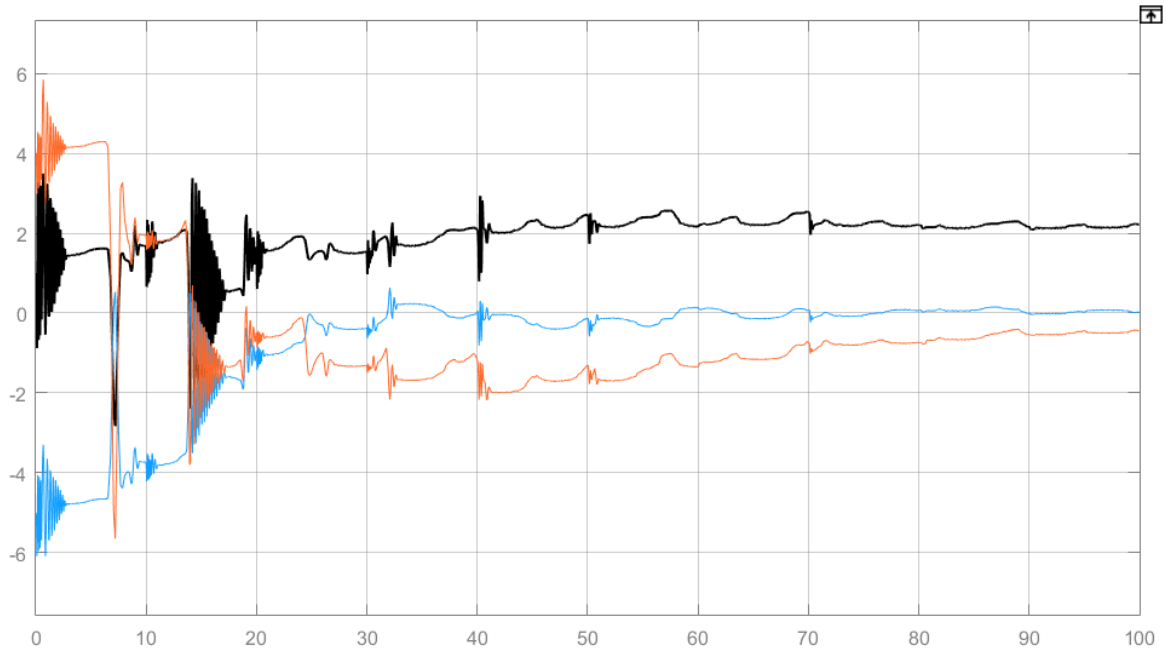

Рис. 6. Графики, показывающие процесс идентификации коэффициентов функции $f_м(x)$, нижний (красный) график - $a_{м_1}$(стремится к 0), верхний (черный) - $a_{м_3}$(стремится к 2), средний (синий) - $a_{м_2}$ (стремится к 0)

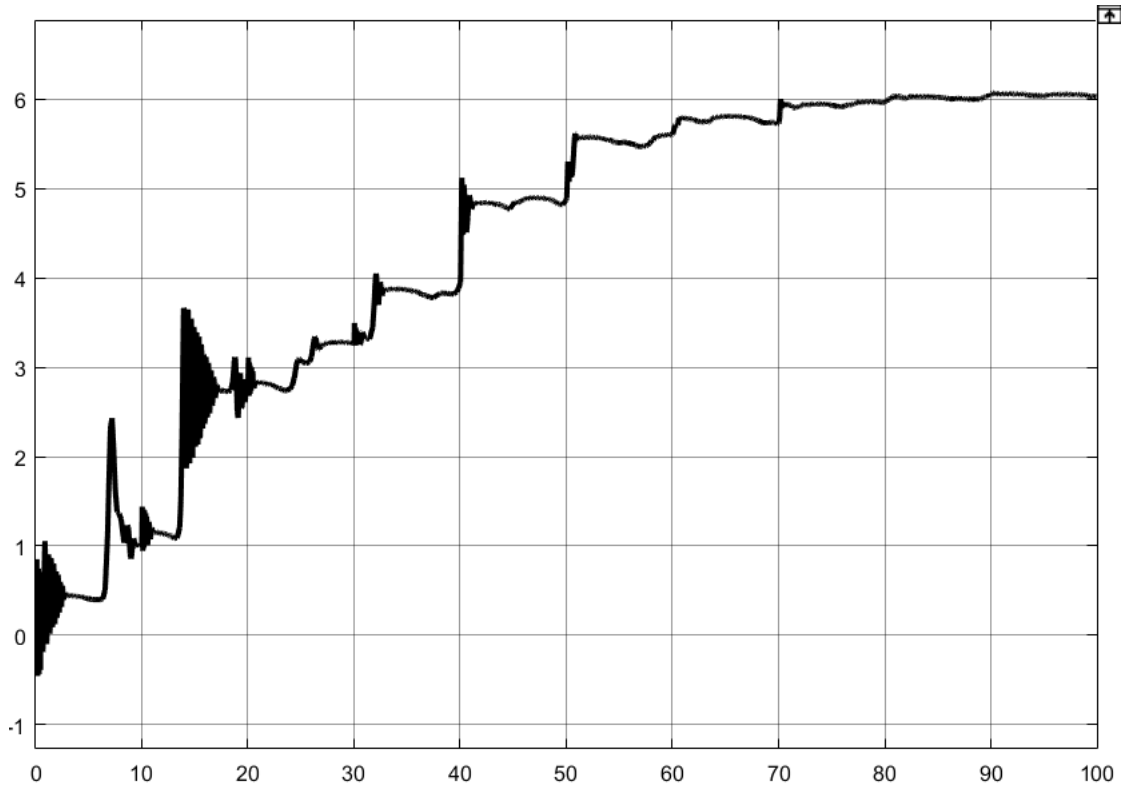

Рис. 7. График настройки коэффициента модели $К_м$, стремится к значению коэффициента управления ОУ К=6.

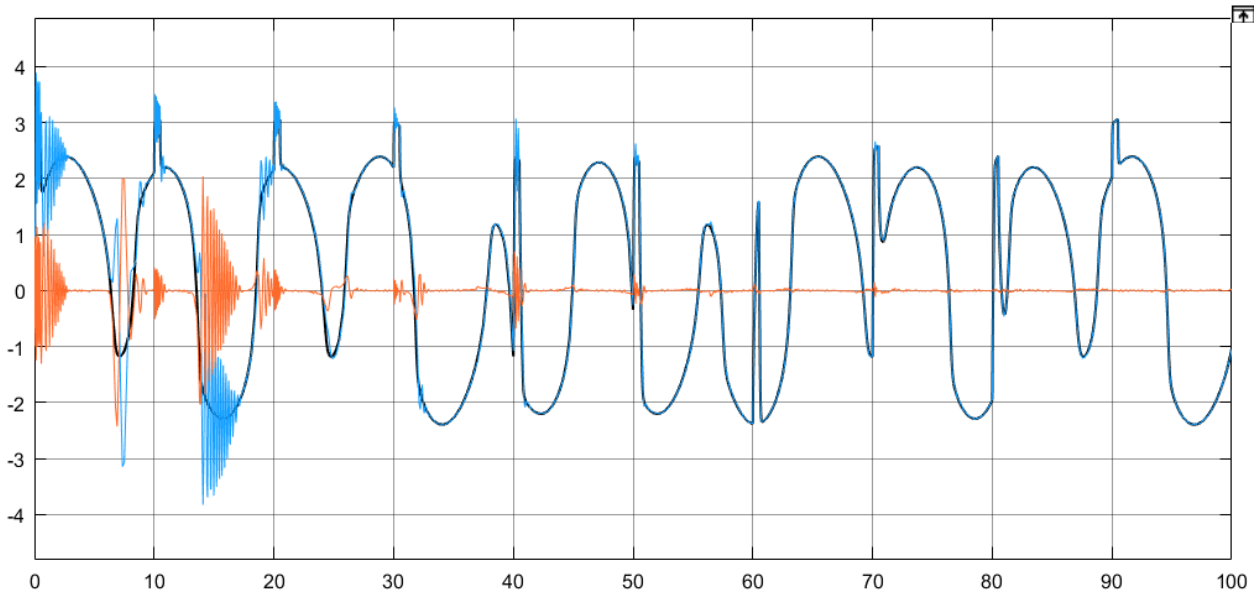

Рис. 8. Графики настройки сигналов модели (x_d) – черный график, объекта ($\mathbf{x}$) – синий график, их разницы ($\mathbf{e}$) (ошибки настройки сигналов) - красный график.

Если f(x) = 2x, получаем графики настройки коэффициентов, изображенные на рисунках 9-11.

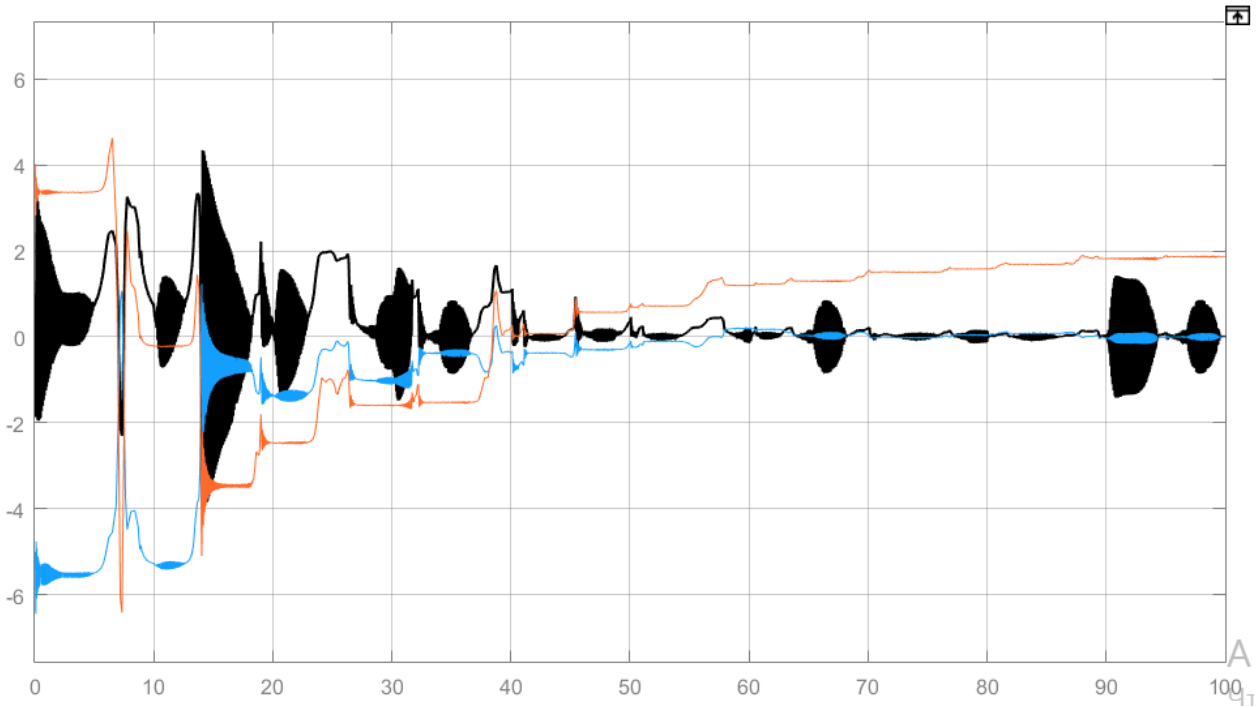

Рис. 9. Графики, показывающие процесс идентификации коэффициентов функции $f_м(x)$, верхний (красный) график - $a_{м_1}$(стремится к 2), средний (черный) - $a_{м_3}$(стремится к 0), нижний (синий) - $a_{м_2}$ (стремится к 0).

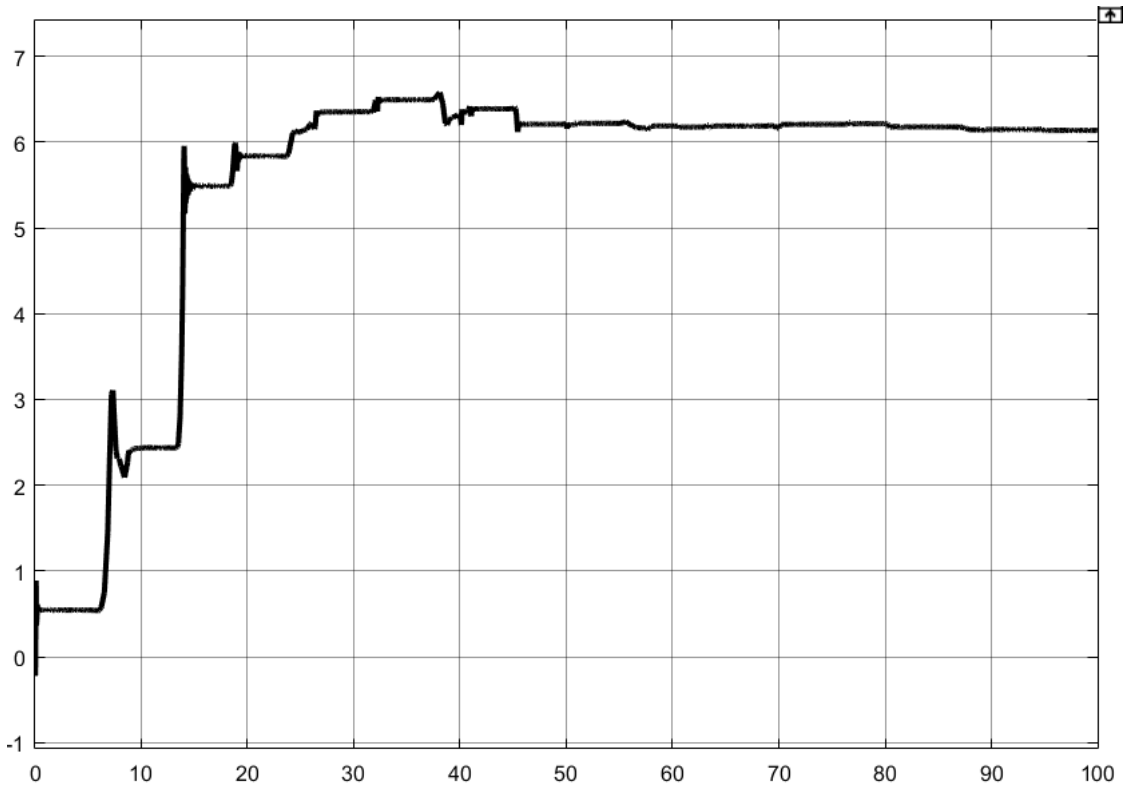

Рис. 10. График настройки коэффициента модели $K_м$

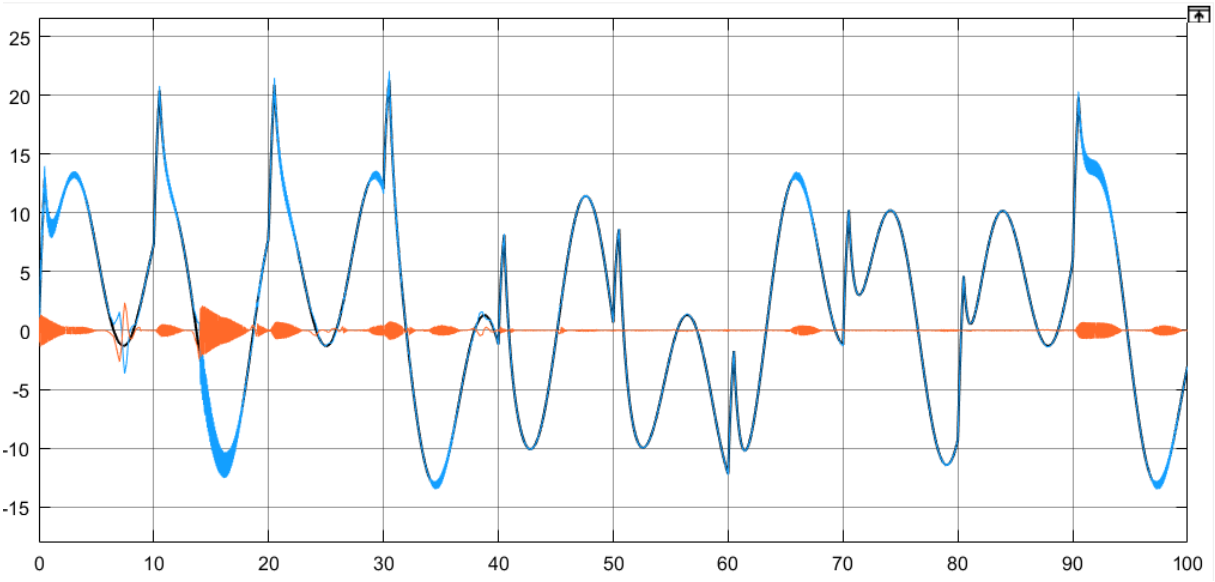

Рис. 11. Графики настройки сигналов модели (x_d) – черный график, объекта (x) – синий график, их разницы (e) (ошибки настройки сигналов) - красный график

Так как $f(x) = 2x$ – линейная функция, а входной сигнал, состоит из четырех гармоник, поэтому настройка сигналов и параметров нелинейная функция с небольшой областью значений вокруг необходимого параметра.

Делая вывод по проведенному эксперименту, мы можем сказать, что данная модель позволяет управлять объектом с заранее неизвестными параметрами и настраивать управление (адаптировать) при изменении параметров.

Список литературы:

1. Андриевский Б.Р., Фрадков А. Л. Избранные главы теории автоматического управления : СПб : Наука, 2000. 475 с.
2. Дыда А. А., Адаптивное и нейросетевое управления сложными динамическими объектами : Владивосток : Дальнаука, 2006. 149 с.
3. Дыда А.А., Чинчукова Е.П., Воробьева С.А., Построение робастно-устойчивой системы управления курсом судна, Научные проблемы транспорта Сибири и Дальнего Востока. 2011 № 1. С. 107-111.
4. Ким Д.П., Теория автоматического управления. Т. 1. Линейные системы. - М. : ФИЗМАТЛИТ, 2003. - 288 с.
5. Чинчукова Е. П., Устойчивость системы управления морскими подвижными объектами с параметрической неопределенностью, Сборник докладов 58-й международной молодёжной научно-технической конференции, посвященной 120-летию морского образования в Приморском крае. 2010. Том 1. С. 107..
6. Чинчукова Е.П. Адаптивно-робастное управление объектами со структурно-параметрической неопределенностью, Сборник докладов 59-й международной молодёжной научно-технической конференции,. 2011. Том 1. С. 178..
7. Andrey Ross, Thor I. Fossen, Tor Arne Johansen, Identification of underwater vehicle hydrodynamic coefficients using free decay test, IFAC 2004. P. 363-368.
8. Nomoto, K., Taguchi, K., Honda, K. and Hirano, S., “On the Steering Quality of Ships,” International Shipbuilding Progress, Vol. 4, pp. 354-370 (1957).
9. Norrbin, N.H., “On the Design and Analysis of the Zig-Zag Test on Base of Quasi-linear Frequency Response,” Technical Report No. B140-3, The Sweden State Shipbuilding Experimental Tank (SSPA), Gothenburg, Sweden (1963).
10. van Amerongen, J., “Adaptive Steering of Ships – A Model Reference Approach to Improved Maneuvering and Economical Course-Keeping,” Ph.D. Thesis, Delft University of Technology, The Netherlands (1982)

УДК 621.321

Шевцов Александр Васильевич,
доцент кафедры АСИБ, МГУ им. адм. Г.И. Невельского

ИНФОРМАЦИОННЫЕ АСПЕКТЫ ВТОРОГО ЗАКОНА ТЕРМОДИНАМИКИ

В статье обсуждается связь понятий *количества информации* и *физической энтропии*. Необходимость в последнем из этих понятий появилась при необходимости дать количественную формулировку второго закона термодинамики, который запрещает в изолированной системе процессы, сопровождающиеся увеличением энтропии.

В термодинамике под изолированностью системы понимается как невозможность передачи энергии этой системе в виде механической работы ($dA = 0$) или тепла ($dQ = 0$), и если первое легко достижимо, то второе выполнимо лишь в идеале с привлечением понятия *термостата*. Обычная

формулировка второго закона разрешает в такой системе лишь те процессы, в которых суммарная энтропия не уменьшается:

$$dH \geq 0. \qquad (1)$$

Иными словами, утверждается, что в изолированной в тепловом смысле термодинамической системе невозможно переведение тепловой энергии в механическую работу без передачи части тепловой энергии «холодильнику» (т. е. с использованием термостата) – невозможен *вечный двигатель второго рода*[1].

Однако легко представить себе ситуацию, когда, в дополнение к сказанному, возможен приток информации *dI*о системе, т.е. если физическая система является изолированной лишь в *тепловом*, но не *информационном* отношении.

Связь физической и информационной энтропий [1], [2], [3] приводит к мысли о необходимости обобщить закон (1), заменив его условием неубывания суммы энтропии и информации:

$$dH + dI \geq 0. \qquad (2)$$

Следовательно, если имеется приток информации, то можно тепловую энергию системы (без помощи «холодильника») превратить в механическую.

Другими словами, возможен *вечный двигатель второго рода*, питающийся информацией.

Мысли о возможности описанного выше обобщения второго закона термодинамики на случай систем с притоком информации возникли давно в связи с обсуждением мысленной конструкции, называемой «*демоном Максвелла»*[2]. Данный персонаж исполняет функции привратника, открывая или закрывая дверцу в непроницаемой перегородке, разделяющей сосуд с газом (в зависимости от скорости подлетающих к ней молекул), что может привести, вопреки второму закону термодинамики, к созданию разности температур или давлений по разные стороны от перегородки не совершая работы. Все энергетические преобразования в такой мысленной модели осуществляются за счёт потока информации о скоростях молекул газа.

Чтобы подробнее разобраться с парадоксом, задаваемым соотношением (2) в наглядной интерпретации «демона Максвелла», рассмотрим описанную выше ситуацию на простых, но позволяющих широкие обобщения, примерах.

Рассмотрим физическую, вообще говоря, динамическую системуS(с термостатом) и связанные с ней координаты x,представляющие часть описывающих её переменных ξ, а также другую физическую системуS_0, которую назовём *измерительным приборами* y – часть её координат η, относящихся к тому же самому моменту времени, что и x. Очевидно, координаты xи yявляются статистически зависимыми случайными величинами, т. е. описываются функциями (плотностями) распределения $p(x)$, $p(y)$,$p(x, y)$.

Для начала предположим, что x – непрерывная координата физической системы, находящейся в состоянии термодинамического равновесия, достигаемого длительным контактом с термостатом. Энергия системы предполагается известной функцией $E(x)$ от этой координаты. Рассмотрим состояние, соответствующее температуре T. В этом случае распределение определяется формулой Больцмана – Гиббса:

$$p(x) = \exp\{[F - E(x)]/T\}, \tag{3}$$

где

$$F = T \ln \int exp[- E(x)/T]\, dx - \tag{4}$$

свободная энергия системы.В данном случае предполагаем, что температура T берётся в энергетических единицах, при которых постоянная Больцмана равна 1. Рассмотрим возможность превращения тепловой энергии в механи-ческую, обусловленную приходом информации о координате x.

Произведём разбиение $\{E_k\}$ пространстваX значений координат x, так что$\sum_k E_k = X$. Поступающая информация указывает, какой области E_kпринадлежит координатаx. При получении такой информации априорное распределение (3) переходит в апостериорное распределение

$$p(x) = \begin{cases} \exp\{[F(E_k) - E(x)]/T\}, & \text{при } x \in E_k, \\ 0, & \text{при } x \notin E_k, \end{cases} \tag{5}$$

где

$$F(E_k) = -T \ln \int_{E_k} e^{-\frac{E(x)}{T}}\, dx - \tag{6}$$

условная свободная энергия. Так как известно, что координата x принадлежит области E_k, её можно окружить непроницаемыми стенками, вводя вместо энергетической функции $E(x)$ функцию

$$E(x|k) = \begin{cases} E(x) & \text{при } x \in E_k, \\ \infty & \text{при } x \notin E_k. \end{cases} \tag{7}$$

Затем медленно раздвигаем стенки, окружающие область E_k, до тех пор, пока они не уйдут в бесконечность. В идеале скорость раздвижения стенок области должна быть бесконечно малой, т. к. только в этом случае этот процесс будет изотермическим (T = const). На стенки действует давление, сила которого при их раздвижении будет совершать работу. Энергия в форме механической работы будет поступать ко внешним телам, механически связанными со стенками. Её величина определяется известным термодинамическим соотношением

$$A = \int pdV, \text{где} p = -\frac{\partial F}{\partial V \partial} \text{ – давление.}$$

Так как, при вариации (расширении) области E_k до $E_k + dE_k$, ко внешним телам переходит механическая энергия

$$dA = (FEk) - F(Ek + dEk) = T\int dEk \exp\left\{\frac{[F(E_k)-F(x)]}{T}\right\} dx. \quad (8)$$

В силу медленности рассматриваемый процесс протекает изотермически, т. е. без изменения температуры. Это происходит вследствие притока тепловой энергии из термостата, контакт с которым не должен прерываться. Тогда источником уходящей из системы механической энергии будет тепловая энергия термостата, превращающаяся в механическую работу. Чтобы подсчитать полную работу A_k, нужно просуммировать дифференциалы (8). При уходе стенок в бесконечность область E_k совпадает со всем пространствомX, а свободная энергия – с (4). Поэтому полная работа равна разности свободных энергий (4)и(6)

$$Ak = F(Ek) - F \quad (9)$$

Если проинтегрировать (3) по E_k, то получим $P(E_k)$, а аналогичный интеграл от (5) равен единице, т. е.

$$\exp\left\{\frac{[F(E_k)-F(x)]}{T}\right\} = P(Ek) \quad (10)$$

Учитывая это соотношение, из (9) получаем

$$Ak = -T \ln P(Ek) = T H(|\, Ek), \quad (11)$$

где $H(|\, E_k)$ – условная энтропия.

Так как полученное соотношение соответствует тому, что точка xс вероятностью $P(Ek)$ принадлежит области E_k, то, усредняя (11) по всем областям, находим среднюю энергию, превратившуюся из тепловой формы в механическую:

$$A = \sum_k A_k \mathrm{P}(E_k) = TH_{E_k} \quad (12)$$

Это соотношение следует, в общем случае, дополнить знаком неравенства, учитывая относящееся к неравновесному (протекающему недостаточно медленно) процессу, т. е.

$$A \leq TH_{E_k} \quad (13)$$

Полученное соотношение позволяет утверждать, что максимальное количество тепловой энергии, переходящее в работу равно произведению абсолютной температуры на больцмановское количество информации. Иными словами, *приток информации о физической системе позволяет переводить тепловую энергию в работу без передачи части тепловой энергии холодильнику.* Утверждение второго закона термодинамики о невозможности такого процесса справедливо лишь при отсутствии притока информации.

Рассмотренный выше пример можно обобщить на более сложные ситуации, когда информация не сводится к указанию области принадлежно-

сти E_k, а носит более сложный характер. Такая ситуация имеет место, если номер области, содержащейx, указывается с ошибкой ($\acute{k}$ вместо k). В этом случае количество поступающей информации определяется шенноновской формулой:

$$I = H_{E_k} - H_{E_{\acute{k}}},$$

что меньше, чем ранее рассмотренная энтропия H_{E_k}.

Ещё более общая ситуация имеет место в случае, когда информация о значении x может поступать не в виде номера области, а в виде какой-то другой случайной величины y, статистически связанной с x. Количество информации в этом случае также определяется формулой Шеннона:

$$I = H_x - H_{x|y} \tag{14}$$

Апостериорное распределение $p(x|y)$ будет иметь более сложную форму, чем (5), тем не менее, обобщённый второй закон термодинамики будет иметь прежний вид (2), если под I понимать количество информации, определяемое (14). Соотношение (13) при этом следует заменить формулой

$$A \le TI \tag{15}$$

Действительно, если рассмотреть бесконечно медленный изотермический переход от состояния, соответствующему апостериорному распределению $p(x|y)$ и имеющего энтропию $H_{x|y}$, к первоначальному (априорному) состоянию с заданным распределением p (x) . Этот переход должен проходить в соответствии со вторым законом термодинамики (1), который можно записать в виде $dH_T + dH_x \ge 0$, или $TdH_x - dQ$,где dH_Tи dH_x – изменения энтропий термостата и системы при передаче от термостата системе количества теплоты $dQ = -TdH_T$. По первому закону термодинамики $dA = dQ - dU$, где $U = \boldsymbol{M}E_x -$ внутренняя энергия системы, связанная со свободной энергией F известным соотношением $U = F + TH_x$. Дифференцируя последнее, имеем $dF = dU - TdH_x$, и сопоставляя со вторым законом термодинамики получаем формулу для элементарной работы

$$dA \le -dF \tag{16}$$

Суммируя элементарные работы (16) получаем, что каждому наблюдённому значению y соответствует работа

$$A_y \le - F + F(y) \tag{17}$$

Здесь F – свободная энергия (4), а $F(y)F(y)$ – свободная энергия

$$F(y) = \boldsymbol{M}[E(x)|\, y] - T\, H_x(|\, y) \tag{18}$$

(соответствующая апостериорному распределению $p(x|y)$, полагающаяся равновесной). Подставляя (18) в (17) и усредняя по y,с учётом соотношения $F = \boldsymbol{M}E(x) - T\, H_x$, получаем $A \le T(H_x - H_{x|y})$, что эквивалентно (15).

Рассмотренное в (2) обобщение второго закона термодинамики никоим образом его не отменяет. *Вечный двигатель второго рода – невозможен*, т. е. невозможно создание устройства, соединяющего автоматический измеритель с информационным преобразователем тепловой энергии в механическую. Это утверждение приводит к заключению о необходимости энергетических затрат при получении и записи информации о физической системе. Конкретно, если система находится при температуре T, то для получения и записи количества информации dI о ней необходимо потратить как минимум TdI энергии, взятой извне, по отношению системы с термостатом[3].

Для доказательства этого вернёмся к заданным в начале элементам и их характеристикам общего комплекса физической системы с термостатом и измерительной системы. В дополнение к ранее сделанным введём следующие обозначения:H_+ – энтропия комбинированной системы S, H_T – энтропия термостата, $I_{\xi\eta} \geq I_{xy}$– общее количество информации, получаемое при совместном функционировании системно-записывающего комплекса (максимальное количество информации, которое данная записывающая система может получить и передать самой системе; очевидно, равенство достигается лишь в случае, когда координаты x и yфункционирования систем S и S_0 полностью совпадают с координатами ξ и η их описания).

Назовём *нормальным физическим записыванием информации* физический процесс, протекающий при взаимодействии систем S и S_0между собой и, возможно, также с другими системами, при котором первоначальное состояние, характеризуемое совместным мультипликативным распределением $p_1(\xi)\times p_2(\eta)$ переходит в конечное состояниеp (ξ,η)с теми же парциальными распределениями $p_1(\xi)$ и $p_2(\eta)$. До начала записывания и после него системы S и S_0предполагаются невзаимодействующими.

Второй закон термодинамики, применённый к процессу записывания информации, имеет вид:

$$\Delta H_+ + \Delta H_T \geq 0 \tag{19}$$

При этом изменение энтропии системы с термостатом, очевидно, равно

$$\Delta H_+ = H_{\xi\eta} - H_\xi - H_\eta = -I_{\xi\eta}. \tag{20}$$

Термостату в итоге передана энтропия$\Delta H_T \geq I_{\xi\eta}$и, следовательно, должна быть отдана тепловая энергия $A \geq T\, I_{\xi\eta}$. Нооткуда она берётся? Ведь по условиям задачи взаимодействие систем S и S_0вначале и в конце отсутствует, так что средняя суммарная энергия комбинированной системыU_+ сводится к сумме средних парциальных энергий собственно системы (с термостатом) и записывающей системы: $U_+ = \boldsymbol{M}E_1(\xi) + \boldsymbol{M}E_2(\eta)$. Они же остаются неизменными вследствие неизменности парциальных распределений $p_1(\xi)$ и $p_2(\eta)$. Итак $\Delta U_+ = 0$ и, следовательно, энергия A должна быть взята в процессе записывания информации *извне от каких-то внешних источников нетепловой информации.*

Таким образом, можно сформулировать основное утверждение:

Если нормальное физическое записывание информации протекает при контакте с термостатом, имеющем температуру T, то для его осуществления необходимо потребление и передача термостату (в виде теплоты) энергии

$$A \geq I\,T, \tag{21}$$

где

$$I = H_x + H_y - H_{xy} \tag{22}$$

– шенонновское количество информации.

Сопоставляя теперь неравенства (15) и (22) видно, что кажущееся нарушение второго закона термодинамики для информационно неизолированных физических систем проистекает от игнорирования статистико-термодинамических процессов в системе измерения и передачи информации, контактирующей с физической системой с термостатом. При рассмотрении комплекса этих систем никакого нарушения второго закона термодинамики нет.

Список литературы

1. Д. В. Сивухин. Общий курс физики. Т. 2. Термодинамика и молекулярная физика [Текст]. М. : Наука, главн. ред. физ.-мат.лит-ры, 1975, – 552 с.

2. Р. Л. Стратонович Элементы молекулярной физики, термодинамики и статистической физики [Текст]: учеб пособие / Стратонович Р. Л., Полякова М. С. – М. : Изд-во Моск. ун-та, 1981. – 176 с.

3. Р. Л. Стратонович Теория информации [Текст]. М.: Сов. радио, 1975, – 424 с.

УДК 621.321

Шевцов Александр Васильевич,
доцент кафедры АСИБ, МГУ им. адм. Г.И. Невельского

ОДИН ПОДХОД К ЗАДАЧЕ ШКАЛИРОВАНИЯ ИНФОРМАЦИОННЫХ МЕР И МЕТРИК

При решении целого ряда задач в биологии, геологии, экологии и техники, т. е. в различных разделах естествознания [1], [2], [3], и не только [4], при необходимости построения математических моделей, встает задача оценки статистически-информационной значимости полученных результатов. Кроме того, может требоваться оценка разнообразия состояний изучаемых систем или независимости и достаточности выбранных для их описания наборов признаков и т. п. Для решения таких задач, помимо стандартных статистических методов, иногда используются различные информационные меры и метрики.

Возможность такого применения информационных функций обуславливает к ним несомненный интерес. Однако в литературе по теории информации, более того, в той её части, что обычно называют «приклад-

ной теорией информации», очень мало работ, в которых были бы представлены большинство информационных функций, рассмотрены их свойства и дана наглядная геометрическая интерпретация соотношениям между ними. В некоторой степени этот недостаток восполнен в [5].

Кроме того, существует проблема интерпретации и самих этих функций, и полученных с их помощью результатов, в сложившихся технических представлениях или в соответствии с данной конкретной областью приложения.

Проблема прежде всего в том, что не уделялось должного внимания разработке методик оценки эффективности как на этапе выбора информационных мер и/или метрик так и при анализе результатов при их использовании, в отличие от практики применения статистических методов в аналогичных задачах. Любая статистика, коэффициент корреляции или сходства в задачах статистического анализа подчинён, хотя бы и асимптотически, одному из небольшого числа хорошо исследованных и давно табулированных законов распределения. Это позволяет статистически оценить и уровень значимости достигнутых результатов, и размер возможной ошибки, а хорошо проработанный раздел той же статистики позволяет ориентироваться при выборе наиболее статистически устойчивых и эффективных статистик и критериев их применения. Почти ничего подобного не существует для информационных функций и конструируемых из них отдельными авторами мер и метрик, хотя все информационные функции, как и статистики, основаны на вероятностных мерах вполне конкретных распределений, но сказать что-либо о распределении этих функций довольно затруднительно.

Сказанное выше позволяет предложить следующий практический способ унификации, калибровки и/или шкалирования информационных мер, могущих использоваться наряду или вместо статистических в соответствующих задачах. Рассмотреть параллельно применение тех и других на одном и том же статистическом материале и сопоставлен результатов.

Итак, на основании числового выборочного материала необходимо провести проверку на «близость» этих выборок, используя как классические статистические методы, так и с использованием некоторых информационных мер. При этом *статистическая близость* проверяется как по генеральной совокупности с одной стороны, так и их статистической зависимости с другой. То есть, либо выборки контролируются одним и тем же законом распределения, либо описывающие их законы распределения достаточно заметно связаны. Предполагается, что сконструированные на основе этих же распределений информационные меры достаточно значимо прореагируют на наличие или отсутствие такой близости или связи, что, в свою очередь, позволит их откалибровать.

При этом высокая корреляция подтверждает однородность выборок, а задаваемый при статистических исследованиях вариационных рядов уро-

вень «значимости» (уровень «доверия») даёт возможность шкалировать соответствующие информационные меры.

1. Информационное сопоставление заданных выборок проводится по следующим информационным мерам:

1.1. Применяя «информационное расхождение» – *дивергенцию Кульбака* [6]

$$\sum_{k=1}^{n}[p_i(x_k) - p_j(x_k)] \times \log\frac{p_i(x_k)}{p_j(x_k)}, \qquad (1)$$

где $p_i(x_k)$ и $p_j(x_k)$ – сопоставленные каждому k – му элементу выборок A_i и A_j вероятности (сумма этих вероятностей по всем элементам равна 1 для каждой выборки).

Указание 1. Так как исходные данные могут представлять собой точечные числовые выборки без каких-либо соответствующих вероятностей или хотя бы возможностей частотного представления, то их необходимо предварительно *рандомизировать*, т. е. просуммировать все элементы в каждой выборке, а затем разделить каждый элемент соответствующей выборки на её сумму. Полученный набор величин $\{p_i(x_k)\}$, k =1 ÷ n даёт требуемые вероятности выборок $\{A_i\}$.

1.2. Применяя информационную метрику Вайса [4], [7] – субъективную оценки близости двух исходов (выборок) A_i и A_j :

$$d(A_i, A_j) = \sum_{k=1}^{n} d_k^{ij} = \sum_{k=1}^{n}(1 - |x_k^i - x_k^j|), \qquad (2)$$

где $\{x_k^j\} = A_j$, $\{x_k^i\} = A_i$. Величины $\{x_k^j\}$ и $\{x_k^i\}$ – это те же величины $\{p_i(x_k)\}$и $\{p_i(x_k)\}$, но упорядоченные по возрастанию или убыванию.

1.3. Применяя информационные меры, рассмотренные в [5]:

а. *Метрика Шеннона*

$$\mathrm{d}(x, y) = H(x \mid y) + H(y \mid x). \qquad (3)$$

Приведённая функция не является метрикой в полном смысле этого понятия, так как для неё не выполняется свойство $\mathrm{d}(x, y) = 0 \rightarrow x = y$, т. е. функция $\mathrm{d}(x, y)$ – псевдометрика. Однако, отождествляя все пары (x,y) из ансамбле (X,Y) с $\mathrm{d}(x, y) = 0$, то есть рассматривая классы эквивалентности, получим полноценную метрику, заданную на этих классах.

При этом справедливо свойство

$$\mathrm{d}(x, y) = 0 \leftrightarrow H(x) = H(y) = H(x, y). \qquad (4)$$

б. Рассмотреть следующую функцию, также удовлетворяющую аксиомам метрики:

$$\Phi_1(x, y) = \frac{H(x \mid y) + H(y \mid x)}{H(x, y)}. \qquad (5)$$

Обе предлагаемые метрики являются мерами близости точек, представляющих ансамбли X и Y в n-мерном гиперпространстве

Предлагается также рассмотреть информационные меры и безразмерные относительные меры *взаимозависимости* и *взаимной независимости* (по аналогии с понятиями *сходства* и *различия*, используемыми во многих прикладных задачах) двух или нескольких вероятностных ансамблей.

в. Рассмотреть *меру взаимозависимости* в виде

$$\mathcal{E}(x, y) = H(x) + H(y) - \mathrm{d}(x, y) = 2\, I(x, y). \tag{6}$$

Функция $\mathcal{E}(x, y) = 0$, если X и Y взаимно независимы и наоборот. Если X и Y связаны функциональной зависимостью, то

$$\mathcal{E}(x, y) = \mathcal{E}_{max}(x, y) = 2\, H(x) = 2\, H(y) = 2\, H(x, y). \tag{7}$$

Справедливо и обратное утверждение.

г. Говоря о взаимозависимости и о взаимной независимости 3, 4, …, n вероятностных ансамблей рассмотреть соответствующие меры:

$$\mathcal{E}(x^{(1)}, \ldots, x^{(n)}) = n\,(T - S), \tag{8}$$

$$D(x^{(1)}, \ldots, x^{(n)}) = n\,S - T, \tag{9}$$

где

$$T = \sum_{i=1}^{n} H(x^{(i)});\; S = H(x^{(1)}, \ldots, x^{(n)}). \tag{10}$$

Функция $D(x^{(1)}, \ldots, x^{(n)})$ при $n = 2$ есть метрика Шеннона.

д. Рассмотреть также относительные меры взаимозависимости и взаимной независимости:

$$K_0(x^{(1)}, \ldots, x^{(n)}) = \frac{n(T-S)}{(n-1)T} = \frac{n[\sum_{i=1}^{n} H(x^{(i)}) - H(x^{(1)}, \ldots, x^{(n)})]}{(n-1)\sum_{i=1}^{n} H(x^{(i)})}, \tag{11}$$

$$\Phi_0(x^{(1)}, \ldots, x^{(n)}) = \frac{nS-T}{(n-1)T} = \frac{nH(x^{(1)}, \ldots, x^{(n)}) - \sum_{i=1}^{n} H(x^{(i)})}{(n-1)\sum_{i=1}^{n} H(x^{(i)})}; \tag{12}$$

в том числе

$$K_0(x^{(1)}, x^{(2)}) = \frac{2I(x^{(1)}, x^{(2)})}{H(x^{(1)}) + H(x^{(2)})};\quad \Phi_0(x^{(1)}, x^{(2)}) = \frac{H(x^{(1)}, x^{(2)}) - I(x^{(1)}, x^{(2)})}{H(x^{(1)}) + H(x^{(2)})};$$

а также

$$K_1(x^{(1)},...,x^{(n)}) = \frac{n(T-S)}{(n-2)T+nS)} = \frac{n[\sum_{i=1}^{n} H(x^{(i)}) - H(x^{(1)},...,x^{(n)})]}{(n-2)\sum_{i=1}^{n} H(x^{(i)}) + nH(x^{(1)},...,x^{(n)})};$$

$$\Phi_1(x^{(1)},...,x^{(n)}) = \frac{2(nS-T)}{(n-2)T+nS)} = \frac{2[nH(x^{(1)},...,x^{(n)}) - \sum_{i=1}^{n} H(x^{(i)})]}{(n-2)\sum_{i=1}^{n} H(x^{(i)}) + nH(x^{(1)},...,x^{(n)})}; \quad (13)$$

$$K_1(x^{(1)},x^{(2)}) = \frac{I(x^{(1)},x^{(2)})}{H(x^{(1)},x^{(2)})}; \quad \Phi_1(x^{(1)},x^{(2)}) = \frac{H(x^{(1)},x^{(2)}) - I(x^{(1)},x^{(2)})}{H(x^{(1)},x^{(2)})}.$$

Следует отметить, что предложенные информационные меры в полной мере аналогичны мерам сходства, различия и корреляции, используемых в различных прикладных статистических задачах, могут быть метриками или не быть таковыми, на их основе можно проводить классификацию объектов и явлений. Перспективно применение таких мер в задачах на системах, с имеющими там место *отношениями толерантности*.

2. Статистическое сопоставление заданных выборок проводится по следующим критериям [8]:

2.1. Критерий Колмогорова – Смирнова.

Нулевая гипотеза H_0: $\{p_i(x_k)\}=\{p_i(x_k)\}$ против альтернативной гипотезы H_1: $\{p_i(x_k)\} \neq \{p_i(x_k)\}$; критическое множество (те значения критерия, при которых отвергается нулевая гипотеза)

$$K(A_i\,,\,A_j) = \{\sqrt{\frac{mn}{m+n}} D_{m,n} \geq q\}, \text{ где } D_{m,n} = \max_{x_k} |p_i(x_k) - p_j(x_k)|, \quad (14)$$

где m и n – объёмы выборок A_i , A_j , критическое значение q – корень уравнения $K(q) = 1 - \varepsilon$. Функция Колмогорова $K(.)$ – табулирована, а при m, $n >$ 20 можно для неё использовать аппроксимацию нормальным распределением; ε – уровень значимости данного критерия (она же – вероятность ошибки первого рода: отвергнуть H_0 при её верности); при расчётах рассматривать значения ε = 0,01; 0,02; 0,05; 0,1.

2.2. Непараметрический критерий инверсий Вилкосона.

Объединяют элементы выборок A_i и A_j и элементы полученной объединённой выборки выстраивают по ранжиру (лучше, по возрастанию). Если в полученном ряду некоторому элементу выборки A_i предшествует элемент выборки A_j , то это считается инверсией. Статистика критерия $u_{(i)}$ – общее число инверсий элементов выборки A_i. Кроме этого, по аналогии подсчитывается статистика $u_{(j)}$ – общее число инверсий элементов выборки A_j. При m, $n > 10$ случайная величина u распределена приблизительно нормально с математическим ожиданием Mu = mn / 2 и дисперсией Du = $mn(m+n+1)/12$, поэтому, задаваясь уровнем значимости $q = 1 - \varepsilon$ (ε = 0,01; 0,02; 0,05; 0,1) по таблице стандартного нормального распределения нахо-

дим величины t_q , с помощью которых строим критические области: Mu ± t_q (Du)$^{1/2}$ – вне этой области нулевая гипотеза отвергается; найденные статистики u «примеряют» к рассчитанным критическим областям.

2.3. Ранговые коффициенты корреляции.

3. Рассчитать по тем же экспериментальным данным ранговый коэффициент корреляции Кендалла

$$\tau = \frac{2S}{n(n-1)} = \frac{S}{\sqrt{\left[\frac{n(n-1)}{2}-u_i\right]\left[\frac{n(n-1)}{2}-u_j\right]}}, \qquad (15)$$

где $S = P - Q = \sum_{l=1}^{n}\sum_{s=l+1}^{n} \mathrm{sign}\left(k_{(i)l} - k_{(j)s}\right) = 2N - \frac{n(n-1)}{2}$;

$sign(a-b) = \begin{cases} 1, a > b, \\ 0, a < b; \end{cases}$ здесь P – суммарное число наблюдений следующих за текущими наблюдениями с *большим значением рангов* для выбранной выборки A_i или A_j; Q – суммарное число наблюдений следующих за текущими наблюдениями с *меньшим значением рангов* для выбранной выборки; $k_{(i)l}$ и $k_{(j)s}$ – ранги l-го элемента выборки A_i и s-го элемента выборки A_j ; N – количество тех пар элементов сопоставляемых выборок, для которых $k_{(j)s} > k_{(i)l}$ при $s > l$, в случае принятия выборки A_i за основу, и наоборот, в случае принятия выборки A_j за основу.

Рассмотренная выше схема расчета не учитывает пары с равными рангами и расчёт коэффициента Кендалла должен вестись по первому равенству в формуле (15); второе равенство в (15) учитывает и равные ранги; при этом $u_i = \Sigma\ t_i\,(t_i - 1)/2$; $u_j = \Sigma\ t_j\,(t_j - 1)/2$, где t_i и t_j – числа «связанных» (одинаковых) рангов рядов A_i и A_j.

4. Рассчитать по тем же экспериментальным данным ранговый коэффициент корреляции Спирмена

$$r_s = 1 - \frac{6S_r}{n(n^2-1)}; \quad S_r = \sum_{r=1}^{n}(k_r - r)^2, \qquad (16)$$

где r – ранги выбранного за основу ряда A_i или A_j , k_r – ранги сопряженных в парах элементов второй выборки.

Расчеты величины корреляции делаются либо по коэффициенту Кендалла, либо по коэффициенту Спирмена (лучше всего рассчитать оба коэффициента). Для определения статистической значимости полученной зависимости (или её отсутствия) предлагается воспользоваться тем, что при n >10 справедлива нормальное приближение статистик этих коэффициентов, т.е. они распределены по нормальному закону с нулевыми средними (Mτ = Mr_s = 0) и дисперсиями D$\tau = \frac{2(2n+5)}{9n(n-1)}$; Dr_s = 1/(n – 1). Задаваясь уровнем значимости α = 0,01; 0,02; 0,05; 0,1 определяем по таблице стандартного нормального распределения критические значения, например, коэффициента Спирмена: $r_{s;(1-\alpha/2)} = -r_{s;\alpha/2}$ – нижнее; $r_{s;\alpha/2}$ – верхнее как решение уравнения $1 - \Phi(t_{\alpha/2}) = -r_{s;\alpha/2}/D^{1/2}(r_s) = \alpha/2$.

Для проведения тестовых расчётов использовались группы по четыре выборки. На первом этапе работа проводится со всеми парами из группы заданных выборок; на втором – с группой из трёх, а затем и четырёх.

Пробные расчёты, проводились студентами на практических занятиях как по теории информации, так и по математической статистике и показали почти полную идентичность результатов сравнения выборок как по информационным так и статистическим критериям, предложенным выше. Это позволяет предполагать успешность калибровки и шкалирования рассмотренных информационных критериев на основе сопоставления с результатами параллельного статистического анализа.

Список литературы

1. Азбука теории информации / Кастлер Г. // Сб. Теория информации в биологии. – М. : ИЛ, 1960.

2. Миллер, Р. Л., Кан Дж. С. Статистический анализ в геологических науках [Текст] / Р. Л. Миллер, Дж. С. Кан – М.: Мир, 1965.

3. Теория информации в экологии / Гиляров А. М. //Успехи современной биологии. Т. 64, вып. 1 (4), 1967.

4. Темников, Ф. Е. Теоретические основы информационной техники [Текст] / Ф. Е. Темников, В. А. Афонин, В. И. Дмитриев. М. : Энергия, 1971, – 424 с.

5. К вопросу формирования и применения информационных мер и метрик / А. В. Шевцов // Вестник Морского государственного универси-тета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток : Мор. гос. ун-т, 2013. – Вып.

6. Кульбак, С. Теория информации и статистика [Текст]. М. : Наука, Гл. ред. физ.- мат. лит., 1967, – 408 с.

7. Шевцов А.В. Основы теории информации (курс лекций) [Текст] : учеб. пособие. – Владивосток. : Мор. гос. ун-т, 2011. –135 с.

8. Кендалл, М. Дж. Статистические выводы и связи [Текст] / М. Дж. Кендалл, А. Стюарт – М.: Мир, 1973. – 900 с.

УДК 621.391

Шевцов Александр Васильевич,
доцент кафедры АСИБ, МГУ им. адм. Г.И. Невельского

О СЕМАНТИЧЕСКИХ АСПЕКТАХ ТЕОРИИ ИНФОРМАЦИИ

Семантика, в чистом виде, – это *смысловая* сторона языка, отдельных слов и частей слова. И, поскольку, теория информации с момента своего рождения неразрывно связана с понятием *сообщения* (*сигнала*), а также, естественно, с задачами приёма, передачи и хранения этих сообщений, то вопрос семантики информации вполне актуальны. В то же время, созданная К. Шенноном в 1948 г. «Математическая теория связи» [1], которую в дальнейшем стали именовать как «Теория информации» *полностью игнорирует смыл сообщения.*

Обратим внимание на два аспекта теории информации.

Первый аспект связан с тем, что понятие *«информация»*, даже на чисто интуитивном уровне, гораздо шире понятия «*сигнала*», передаваемого или принимаемого в каком угодно виде или в какой удобно форме [2]. Именно поэтому почти сразу за работами Шеннона появились публикации как в развитие предложенных там идей, так и в направлениях, связанных либо с применением этого нового математического аппарата в приложениях весьма далёких от теории передачи сигналов, либо развивающих на основе шенноновских лекал новый подход [3], [4].

Второй, тесно переплетающийся с первым, прямо связан со смысловой составляющей информации и способом её представления.

Имеется множество определений понятия информация от наиболее общего философского: – информация есть отражение реального мира, до наиболее узкого практического: – информация есть все сведения, являющиеся объектом хранения, передачи и преобразования.

Ряд зарубежных авторов трактует информацию с идеалистических позиций как некоторую субстанцию, занимающую промежуточное положение между материей и сознанием.

Но и при материалистической исходной посылке имеется ряд расхождений при конкретизации понятия «информации» по таким существенным вопросам как:

– информация – это свойство конкретного объекта (процесса) или результат взаимодействия объектов (процессов)?,

– информация присуща всем видам материи или лишь при её организации определённым образом?,

– информация существует в любых процессах или возникает только в процессах управления?

В работах Колмогорова [5] и Эшби [6] выдвинуто понятие информации как характеристики *внутренней организованности* материальной системы (по множеству её допустимых состояний). Такой подход позволяет оценивать потенциальные возможности систем независимо от процесса передачи или восприятия информации, а также порождает мысль о том, что информация существует независимо от того, воспринимается она или нет. Справедливо, однако, отметить, что проявляться при этом информация может только при взаимодействии объектов (процессов). Н. Винер в своей основополагающей работе по кибернетике остроумно и точно подчеркнул, что «информация есть информация, а не материя и не энергия». В отличие от них информация *может возникать и исчезать*. Так в куске каменного угля содержится информация о событиях, происшедших в далёкие времена, однако она проявляется лишь при взаимодействии с человеком, а при сгорании угля эта информация исчезнет.

Распространённым является также мнение о том, что информация присуща лишь так организованной материи, в которой возможны процессы управления. Тем самым, под информацией подразумевается только то, что воспринято и осмысленно, т. е. то, что целесообразно использовать для

управления. Не говоря уже о субъективизме такого подхода, легко заметить, что вопрос о существовании информации здесь неправомерно сводится к гораздо более узкому вопросу о способности объекта к восприятию и использованию информации.

В качестве квинтэссенции всему вышеизложенному будем полагать, что информация возникает тогда, когда устанавливаются некоторые общие свойства конкретных вещей и явлений, поэтому под информацией можно понимать выделенную сущность, характеристику этих вещей и явлений.
От вопросов трактовки самого понятия «информации» вернёмся к содержательной стороне этого понятия. Слово «информация» по латыни означает *сообщение*, *осведомление о чём-либо*. Для работы с таким материалом как нельзя лучше подходит *семиотика* – наука о знаках, словах и языках. *Знаком* называется условное изображение элемента сообщения, *словом* – совокуп-ность знаков, имеющая смысловое (предметное) значение, *языком* – словарь и правила пользования им. Семиотика анализ знаковых систем проводит, по крайней мере, на трёх уровнях:

1) на *синтаксическом* уровне рассматриваются внутренние свойства текстов, т. е. отношения между знаками, *отражающие структуру данной знаковой системы*;

2) на *семантическом* уровне анализируют отношения между знаками и обозначаемыми ими предметами, действиями, качествами, т. е. *смысловое содержание текста, его отношение к источнику информации*;

3) на *прагматическом* уровне рассматриваются отношения между текстом и теми, кто его использует, т. е. *потребительское содержание текста, его отношение к получателю*.

Таким образом, на семантическом и прагматическом уровнях изучаются внешние свойства текстов

Учитывая определённую взаимосвязь *проблем передачи информации* с уровнями изучения знаковых систем, их также разделяют на проблемы синтаксического, семантического и прагматического уровней, а нередко добавляется ещё так называемый *сигматический* аспект теории информации.

Сигматический аспект отображается теорией сигналов и кодов, рассматривающей условные обозначения элементов информации. Сигналы являются физическими носителями информационных элементов, а коды – обозначениями этих элементов. Таким образом, сигматические оценки не имеют прямого отношения к мерам информации.

Проблемы синтаксического уровня касаются создания теоретических основ построения систем связи с основными показателями функционирования как можно более близкими к предельно возможным, а также совершенствования существующих систем с целью повышения их эффективности. Сюда же относятся чисто технические проблемы совершенствования методов передачи сигналов – материального воплощения сообщений. Иначе говоря, на этом уровне интересуют проблемы доставки получателю со-

общений как совокупности знаков при полной абстрагируемости от их смыслового и прагматического содержания [7]. Именно решением задач этого ряда занимается традиционная современная теория информации. При этом она опирается на понятие «количества информации», являющееся мерой частоты употребления знаков, которая никак не отражает ни смысла, ни важности передаваемых сообщений. Структурная мера Хартли, вероятностная мера Шеннона и другие статистические оценки количества информации относятся к синтаксическому аспекту. Таким образом, можно сказать, что традиционная теория информации находится на синтаксическом уровне.

На прагматическом уровне интересуют последствия от получения и использовании информации абонентом. Проблемы этого уровня – это проблемы эффективности и основная сложность здесь состоит в том, что *ценность* или потребительская стоимость информации может быть совершенно различной для различных получателей, а также существенно зависеть от *истинности* и *прогностичности* информации, *своевременности* её *доставки* и использования. Задержки в доставке или использовании информации могут иметь катастрофические последствия в связи с тем, что управляющие воздействия должны осуществляться в реальном масштабе времени, т. е. со скоростью изменения состояния управляемых объектов или процессов.

Таким образом, прагматический аспект теории информации в основном связан с проблемами объективного и универсального подхода к определению т. н. «ценности» информации [8], [9], а также с вытекающими из этого задачами борьбы со *старением* информации (своевременность доведения информации), что можно понимать, как *потерю её ценности в процессе доставки* [10]. Работа в направлении количественного определения прагматического содержания информации на настоящий момент проделана большая, однако рассмотренные подходы к проблеме ценности информации обладают заметной долей эвристических элементов. Наиболее формализованы подходы, опирающиеся на минимизацию штрафов [9], хотя и здесь выбор функции штрафов нередко представляет собой эвристический акт. Ещё менее формализованным является подход, исходящий из максимизации выигрыша [8]. Обычно достаточно чётко осознаваемый выигрыш часто требует немалых трудов для того, чтобы явно выразить его в количественной, функциональной или алгоритмической форме; этот процесс в значительной мере является эвристическим.

Естественно поэтому, что *субъективные* аспекты ценности информации в принципе не могут не быть существенно эвристическими и даже интуитивными, поскольку речь идёт о проблемах, касающихся поведения и субъективных оценок, относящихся к человеческой личности. Это конечно не умаляет значение попыток формализовать этот аспект ценности информации, однако не позволяет считать разработанные меры достаточно конструктивными для широкого практического применения.

Интересующие нас в данной работе проблемы семантического уровня связаны с формализацией смысла передаваемой информации, например, введением количественных оценок близости информации к истине, т. е. оценок её качества. Эти проблемы чрезвычайно сложны, т. к. смысловое содержание информации больше зависит от получателя, чем от семантики сообщения, представленного в каком-либо языке (хотя бы и в формальном). Информация заложена в сообщении, но проявляется она только при взаимодействии с получателем, например, потому, что она может быть зашифрована. Так, если получатель – человек, то и незашифрованное (или правильно расшифрованное) сообщение может быть понято по-разному. В частности, из полученной телеграммы адресат может извлечь совершенно другую информацию по сравнению с той, которая будет доступна работнику телеграфа. Основная причина состоит в том, что различное понимание того или иного слова может сильно изменить смысл переданной информации. Кроме того, в семантическом аспекте информации наиболее силён человеческий фактор – восприятие человеком информации зависит от его эмоционального состояния, накопленного жизненного опыта и многих других факторов.

Следует отметить, что всё ещё не предложено достаточно последовательных и универсальных методик измерения семантической информации, а имеющие место подходы к решению этой задачи носят весьма частный характер.

Необходимо также отметить, что в инженерных приложениях *прагматические* оценки сливаются с *семантическими*, поскольку не имеющие смысла сведения бесполезны, а бесполезные сведения бессмысленны.

В качестве семантических мер информации предложены следующие: *содержательность*, *целесообразность* и *существенность* информации.

Оценка эффективности логического вывода, степени приближения к истине требует некоторой формализации, в данном случае – формализации смысла. Один из путей такой формализации предлагается семантической теорией информации. Её основоположники Карнап и Бар-Хиллел предложили [11] использовать в целях измерения смысла функции истинности и ложности логических высказываний. За основу дискретного описания объекта берётся «атомарное» (неделимое) предложение, подобное элементарному событию теории вероятностей и соответствующее неделимому кванту сообщения. Полученная таким образом оценка получила название *содержательности* информации.

Рассматриваются две основные меры количества семантической информации в предложении x. Первая мера содержательности информации обозначается *cont* (от английского «content» – содержание). Содержательность события (предложения) x выражается через функцию меры $m(x)$ содержательности его отрицания $(\neg x)$ как

$$cont\,(x) = m(\neg x) = 1 - m(x). \qquad (1)$$

Оценка содержательности основана на математической логике, в которой логические функции истинности $m(x)$ и ложности $m(\neg x)$ имеют формальное сходство с функциями вероятностей события $p(x)$ и антисобытия $q(x)$ в теории вероятностей. В обоих случаях имеют место сходные условия

$$m(x) + m(\neg x) = 1 ; \quad p(x) + q(x) = 1,$$

причём $q(x) = p(\neg x)$. Как и вероятность, содержательность изменяется в пределах $0 \le m(x) \le 1$.

Аналогично сходны статистическое и логическое количества информации. Статистическая оценка количества информации (энтропия)

$$I = \log (1 / p(x)) = - \log p(x). \qquad (2)$$

Вторая, логическая оценка количества семантической информации, получившая обозначение *Inf* (x), имеет сходное выражение

$$Inf(x) = \log [1/(1 - cont(x))] = \log (1/m(x)) = - \log (m(\neg x)). \qquad (3)$$

Отличие статистической оценки от логической в том, что в первом случае учитываются вероятности реализации тех или иных событий, а во втором – меры истинности или ложности событий, что приближает к оценке смысла информации.

Из (3) видно, что логическая оценка семантической информации нелинейно зависит от меры содержательности (1), причём мера *Inf* (x) больше подходит для меры *количества* информации, обладая, в отличии от меры *cont*(x), свойством аддитивности: для логической связки «И» (знак «∧») двух логически независимых предложений x_1 и x_2 справедливы соотношения

$$cont(x_1) + cont(x_2) > cont(x_1 \wedge x_2), \qquad (4)$$

но

$$Inf(x_1) + Inf(x_2) = Inf(x_1 \wedge x_2). \qquad (5)$$

Отметим также – количество семантической информации в сообщении s относительно знаний получателя e определяется следующим образом:

$$Inf(s/e) = Inf(s \wedge e) - Inf(e) = \log_2 \frac{m(s)}{m(s \wedge e)} = \log_2 \frac{1}{m(s/e)}, \qquad (6)$$

где $m(s/e)$ – относительная (условная) логическая вероятность истинности сообщения s при условии истинности знаний получателя e.

Легко заметить, что чисто внешне формулы теории Бар-Хиллела – Карнапа аналогичны формулам теории Шеннона: и здесь и там логарифмы и вероятности, только у Шеннона все вероятности статистические (т. е. эмпирические), а не логические.

Если $m(s \wedge e) < m(e)$, то сообщение s несёт новую информацию получателю, обогащая, таким образом его знания. Если e имплицирует s, то $(s \wedge e)$ эквивалентно e и сообщение s не несёт информации адресату (поскольку в нём нет ничего для него нового). Если выражение $(s \wedge e)$ является противоречием, то $m(s \wedge e) = 0$, что приводит к бесконечному количеству семантической информации. Этот парадокс и невозможность разре-

шения антиномий с условно-ложными предложениями (например, выражение «Луна вращается вокруг Земли и внутри она полая» несёт информацию и дезинформацию одновременно), которые в рамках классической логики теории Бар-Хиллела – Карнапа являются чисто ложными и несут только дезинформацию, привело к тому, что Флориди предложил взамен этой «слабой» теории свою – «сильную» [12].

Он отказался от использования логических вероятностей и заявил, что теория семантической информации не должна быть похожей на теорию Шеннона. В его интерпретации количество семантической информации в сообщении определяется степенью соответствия этого сообщения ситуации (т.е. тому, что происходит в данном месте и в данное время). Несоответствие возникает либо в результате бессодержательности сообщения, либо в результате его неточности. В своей теории Флориди непосредственно не использует понятие дезинформации, вместо этого он вводит понятие *степени неточности* условно-ложных предложений. Степень неточности в условно-ложном предложении s равна:

$$-v(s) = -\frac{f(s)}{l(s)}, \tag{7}$$

где $f(s)$ – число ложных атомарных выражений в s; $l(s)$ – общее число атомарных выражений в s. Для определения истинности атомарных предложений требуется принять принцип априорного всезнания. *Степень бессодержательности* истинного предложения s рассчитывается по формуле:

$$+v(s) = \frac{m(s)}{n}, \tag{8}$$

где $m(s)$ – число миров универсума, в которых s истинно; n – общее число миров универсума (заметим, что, согласно этому определению, величина $+v(s)$ в точности равна величине логической вероятности $m(s)$). Также вводится понятие *функции степени информативности*:

$$i(s) = 1 - v^2(s). \tag{9}$$

Количество семантической информации $i^*(s)$ в сообщении s тогда равно:

$$i^*(s) = \frac{3}{2}\int_{v(s)}^{1}(1-x^2)\mathrm{d}x = 1 - \frac{3v(s)}{2} + \frac{v^3(s)}{2}. \tag{10}$$

Несмотря на все отличия между классической теорией и теорией Флориди, в них есть нечто общее. Если s является истинным предложением, то величина $+v(s)$ равна величине логической вероятности $q(s)$. Мера $i^*(s)$ подобна мере $\mathrm{cont}(s)$, но в отличие от неё, является нелинейной функцией $v(s)$. К сожалению, в теории Флориди нет ничего похожего на меру $\mathrm{inf}(s)$, обладающую замечательным свойством (5) для логически независимых предложений.

Необходимо отметить, что к началу текущего века не только у Флориди, но и у ряда других ученых сформировалось скептическое отношение к индуктивной логике Карнапа. Тем ни менее, поднятая Флориди проблема может быть решена в рамках теории, основанной на логических вероятностях, при соответствующей модификации этой теории.

В работе [13] предлагается модифицировать классическую теорию семантической информации, включив в нее понятие дезинформации, которую несет ложное сообщение. В новой теории, как и в теории Флориди, рассматривается множество различных ситуаций (точек логического пространства-времени). Одно и то же предложение языка может быть истинным в одной ситуации и ложным в другой. Поскольку получатель сообщений не может быть застрахован от ошибок при оценке их истинности, количество семантической информации оценивается отдельно с точки зрения получателя и с точки зрения всезнающего эксперта.

В каждой конкретной ситуации истинное сообщение несет только информацию, а абсолютно ложное – одну только дезинформацию. Условно-ложное предложение s рассматривается как конъюнкция: $s_T \wedge s_F$, где s_T – истинная часть сообщения, s_F – ложная часть сообщения. При этом требуется, чтобы s_T и s_F были логически независимыми (это нужно, в частности, для того, чтобы противоречие не оказалось условно ложным предложением). Тогда *ненормализованные* меры количества *информации* $\mathrm{in}_E(s)$ и количества *дезинформации* $\mathrm{mi}_E(s)$ в условно-ложном предложении s с точки зрения эксперта определяются следующим образом:

$$\mathrm{in}_E(s) = \mathrm{cont}(s_T), \tag{11}$$

$$\mathrm{mi}_E(s) = \mathrm{cont}(s_F), \tag{12}$$

где индекс «E» указывает на соответствие этих мер точке зрения эксперта. *Нормализованные* меры количества семантической информации $\mathrm{inf}_E(s)$ и дезинформации $\mathrm{mis}_E(s)$ в условно-ложном предложении s с точки зрения эксперта:

$$\mathrm{inf}_E(s) = \log_2 \frac{1}{1 - \mathrm{cont}(s_T)} = \log_2 \frac{1}{q(s_T)}, \tag{13}$$

$$\mathrm{mis}_E(s) = \log_2 \frac{1}{1 - \mathrm{cont}(s_F)} = \log_2 \frac{1}{q(s_F)}. \tag{14}$$

Противоречие с точки зрения эксперта несет нулевое количество информации и бесконечное количество дезинформации (бесконечное количество дезинформации означает то, что, если противоречие кому-то покажется истиной, то мир изменится для него до неузнаваемости). Таким образом решается парадокс Бар-Хиллела – Карнапа. Предположим, что получатель информации имеет условно-ложные знания e, эквивалентные конъюнкции: $e_T \wedge e_F$, где e_T – истинная часть его знаний, e_F – заблуждения. Тогда с точки зрения эксперта, получив условно-ложное сообщение s, адресат

реально имеет семантическую информацию и дезинформацию в следующих количествах:

$$\inf_E(s/e) = \log_2 \frac{q(e_T)}{q(s_T \wedge e_T)} = \log_2 \frac{1}{q(s_T/e_T)}, \quad (15)$$

$$\mathrm{mis}_E(s/e) = \log_2 \frac{q(e_F)}{q(s_F \wedge e_F)} = \log_2 \frac{1}{q(s_F/e_F)}. \quad (16)$$

Если получатель воспринимает s как истинное предложение и конъюнкция $s \wedge e$ не является противоречием, то с его точки зрения он получил следующее количество информации:

$$\inf_R(s/e) = \log_2 \frac{1}{q(s/e)} = \inf_E(s/e) + \mathrm{mis}_E(s/e), \quad (17)$$

где индекс «R» обозначает оценку адресата. Очевидно, что точное количество информации (и дезинформации) в пришедшем сообщении может определить только эксперт, а получатель способен лишь на более-менее точные оценки.

Если информация используется в системах управления, то её полезность разумно оценивать по тому эффекту, который она оказывает на результат управления.

Харкевичем [14] была предложена мера *целесообразности* информации, которая определяется как *изменение вероятности достижения цели при получении дополнительной информации*. Полученная информация может быть пустой, т. е. не изменять вероятности достижения цели – в этом случае её мера равна нулю. В других случаях полученная информация может изменять положение дел в худшую сторону, т. е. уменьшать вероятность достижения цели – тогда она будет *дезинформацией*, которая измеряется *отрицательным значением количества информации*. Наконец, в третьем, благоприятном случае, получается добротная информация, увеличивающая вероятность достижения цели и измеряется положительной величиной количества информации.

Мера целесообразности в общем виде может быть аналитически выражена в виде соотношения

$$I_{цел.} = \log p_1 - \log p_0 = \log p_1 / p_0, \quad (18)$$

где p_0 и p_1 – начальная (до получения информации) и конечная (после получения информации) вероятности достижения цели.

Параметрическая информация, может быть представлена трёхмерной моделью, осями координат которой являются параметр X, пространство N и время T, причём под пространством понимается упорядоченное множество источников информации, в частности, измеряемых величин.

Значения величин, точки пространства и моменты времени неравнозначны как сами по себе, так и во взаимных отношениях. Например, наиболее существенны высокие значения давления и температуры в точке выхода газа в момент отрыва ракеты от земли. В других точках и в другие моменты времени эти параметры могут быть несущественны.

Можно различать:

1) существенность самого события;

2) существенность времени совершения события или момент его наблюдения (рано – поздно);

3) существенность места, адреса, номера, локализации, точки пространства, координаты совершения события.

Измерение величины X можно характеризовать несколькими её функциями: вероятности $p(x)$, погрешности измерения $\varepsilon(x)$ и *существенности* $c(x)$. Каждой из этих функций можно поставить в соответствие определённую меру информации. Мерой Хартли оценивается функция погрешности ε при фиксированных значениях функций вероятности и существенности (p = const; c = const). Мерой Шеннона оценивается функция вероятности (p = var) при фиксированных значениях функций погрешности и существенности (ε = const; c = const). Мера существенности информации относится к ситуации с фиксированными функциями погрешности и вероятности (ε = const; p = const). Можно ввести функции существенности c_X, зависящие от величины X, c_T, зависящие от времени T, c_N, зависящие от пространства (канала) N.

Функция существенности отражает степень важности информации о том или ином значении параметра с учётом времени и пространства и должна удовлетворять условию нормировки.

До сих пор при оценке полезности информации не рассматривалась возможность её восприятия и обработки приёмником. Можно рассмотреть полезность информации как от степени новизны, так и от способности приёмника к её восприятию и обработке.

Так Шрейдер [15] полагает, что количество семантической информации в послании любой природы можно оценить как степень изменения системы знаний адресата в результате восприятия сообщения. Следствием потребительского аспекта является дополнение информации понятием *актуации* в смысле активного запроса информации со стороны заинтересованного приёмника. При этом имеется в виду тесная связь между этими понятиями, так как в каждой актуации может содержаться некоторая информация.

Существует три типа вопросов: в одном отсутствует предвосхищение ответа, в другом имеется некоторая доля ответа, в третьем полностью содержится ответ и требуется только его подтверждение. Таким образом, замыкается связь между двумя системами (рис.1): системой S_x , являющейся поставщиком информации, и системой S_y – потребителем информации.

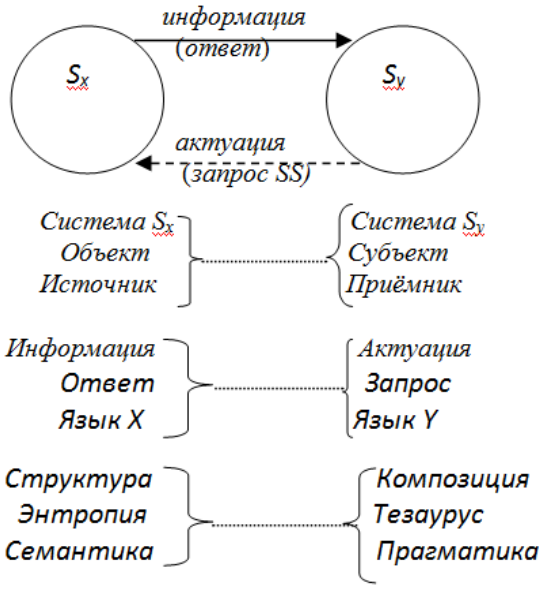

Рис. 1. Обобщённое представление процесса обмена информацией между двумя системами

Целесообразно также использование понятия *тезауруса* (от греческого «сокровищница»), под которым понимается запас знаний, или словарь, используемый приёмником информации. Подобный подход достаточно хорошо разработан и формализован [16], причём его использование выводит задачу оценки и описания информации за рамки чисто семантического аспекта.

С учётом сказанного можно систему извлечения, передачи и приёма информации представить в виде схемы рис. 2.

По схеме источник (объект) обладает определённой энтропией H, которая характеризует способность источника отдавать информацию. Отдача может быть неполной. Информация $I = H_1 - H_2$ поступает в канал, где часть информации теряется или искажается шумом N. Оставшаяся информация достигает приёмника и воспринимается им в той степени, в какой это позволяет сделать тезаурус.

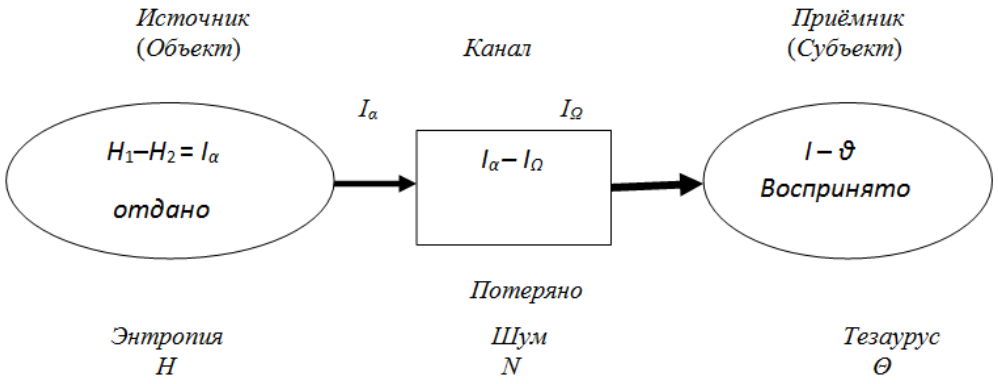

Рис. 2. Схема извлечения, передачи и приёма информации с учётом H, N и Θ

Может оказаться, что, несмотря на высокое богатство структуры и статистики на передающей стороне, приёмная сторона не нуждается в этой информации, так как уже обладает ею, не имеет в ней потребности или просто не умеет с ней обращаться.

Возможна и другая ситуация. Если тезаурус не адекватен передаваемой информации, очень мал или вообще отсутствует, то самая новая и богатая информация не воспринимается, так как она не будет принята приёмником. В тоже время, с приёмом новой информации тезаурус может обогащаться.

Пусть богатство тезауруса оценивается некоторой величиной Θ. Изменение тезауруса под действием сообщения H можно оценить количеством информации $I(H, \Theta)$. Имеется некоторое минимальное количество информации $I_{\min}(\Theta)$ априорной информации $I(\Theta)$ тезауруса в системе S_y, при которой эта система начинает принимать сообщения, поступающие от системы S_x. В силу выпуклости и положительной определённости информации величина $I(H, \Theta)$ возрастает до $I_{max}(H, \Theta)$ при увеличении $I(\Theta)$ до $I_{opt}(\Theta)$, где достигается максимум восприятия. Далее следует спад, обусловленный тем, что априорные знания (тезаурус приёмника) становятся богатыми настолько, что источник не приносит новой полезной информации. При $I(\Theta) = I_{\max}(\Theta)$ восприятие информации прекращается, так как система S_y оказывается насыщенной знаниями в пределах возможностей системы S_x – потенциального источника информации.

Если языки X и Y однозначно определены, то могут быть предусмотрены трансляторы – переводчики $Y \rightarrow X$ и $X \rightarrow Y$, располагаемые в S_X , Sy или и там, и там (совместно). В других случаях возникает проблема взаимопонимания, которая решается методами распознавания и самообучения. При единстве языков возможно непонимание из-за действия помех и искажений.

В схеме на рис. 1 указаны структурные, статистические и семантические характеристики информации: структура, энтропия и семантика на стороне источника S_x; композиция сообщения, в целом тезаурус и прагматика на стороне приёмника S_y.

Композиция отражает те же стороны информационной системы, что структура информации, тезаурус – те же, что энтропия, прагматика – те же, что семантика, хотя связь между этими парами понятий нельзя считать установившейся. Наиболее близкими между собой являются понятия структуры и композиции. Структура как основа исчисления количества информации предполагает дискретное строение и декомпозицию информации, осуществляемые на передающей стороне. Поэтому естественной формой приёмной стороны является композиция, заключающаяся в том, что по возможности восстанавливаются нарушенные связи между элементами информации или воссоздаётся непрерывность информационного комплекса. Иногда это может повлечь за собой переоценку информации.

В качестве краткого резюме: хочется надеяться, что модификация наработанных в прошлом идей и подходов, применение ранее не используемого или создание нового математического аппарата в области семантической информации, может вдохнуть в неё новую жизнь.

Список литературы

1. A Mathematical Theory of Communication. / C. E. Shannon // Bell Syst. Tech. J., 27: – 1948, с. 379-423, 623-656.
2. Управление и информация / А. Е. Мамиконов // Работы по теории информации и кибернетики. – М : 1976.
3. Шрейдер, Ю. А. Сложные системы и космологические принципы. – Системные исследования, 1975 [Текст]. – М. : Наука, 1976.
4. Коган, И. М. Прикладная теория информации. – М. : Радио и связь,1986.– 242 с.
5. Три подхода к определению понятия количества информации / А. Н. Колмогоров // Проблемы передачи информации. – 1965. Т.1. Вып.1, с. 25 – 58.
6. Эшби, У. Р. Введение в кибернетику [Текст]. – М. : ИЛ, 1959. – 354 с.
7. Колесник, В. Д. Курс теории информации / В. Д. Колесник, Г. Ш. Полтыре. – М.: Радио и связь, 1982, – 332 с.
8. О ценности информации /А. А. Харкевич // Проблемы кибернетики. – М. : Физмат-гиз, 1960, № 4.
9. Стратонович, Р. Л. Теория информации [Текст]. – М. : Сов. радио, 1975. – 424 с.
10. Темников, Ф. Е. Теоретические основы информационной техники [Текст] / Ф. Е. Темников, В. А. Афонин, В. И. Дмитриев – М. : Энергия, 1979. – 526 с.
11. An Outline of a Theory of Semantic Information / Y. Bar-Hillel, R. Carnap // Technical Report No. 247, October 27, Research Laboratory of Electronics. – 1952. – 49 с.
12. Outline of a Theory of Strongly Semantic Information / L. Floridi // Minds and Machines, 14(2), 2004, – с. 197-222.
13. Семантическая информация и дезинформации / О. А. Погорелов // Сборник научных статей по итогам V Международной научно-практической конференции «Информатика, Математическое моделирование, Экономика» (г. Смоленск, 11-15 мая 2015 г.), с. 132-143.
14. О ценности информации /А. А. Харкевич // Проблемы кибернетики.– М.: Физматгиз, 1960, № 4.
15. Об одной модели семантической теории информации / Ю. А. Шрейдер // Проблемы кибернетики, в. 13. – 1965, – с. 233-240.
16. Дмитриев, А. К. Основы теории построения и контроля сложных систем / А. К. Дмитриев, П. А. Мальцев. – Л. : Энергоатомиздат. Ленингр. отделение. – 1988. – 192 с.

УДК 004.056.5

Обзор проблем защиты информации в системе «1С: Предприятие» / Р.А. Белоножко, М.В. Мазур // Вестник Морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

В статье приведены и проанализированы проблемы обеспечения информационной безопасности баз данных системы «1С: Предприятие». Особое внимание уделяется клиент-серверной архитектуре хранения данных. Показана перспективность развития систем обеспечения информационной безопасности баз данных «1С:Предприятие».

Ключевые слова: *база данных, информационная безопасность*.

Библиогр.2, ил. 1

УДК 621.311.016.2

Управляемый реактор для автоматического фильтрокомпенсатора / С.И. Борисов // Вестник Морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

В статье рассматривается схема реактированной конденсаторной батареи с управляемым реактором, который используется для автоматической настройки фильтрокомпесатора в резонанс по высшей гармонике тока. Приведены результаты расчета управляемого реактора.

Ключевые слова: *фильтрокомпенсатор, высшие гармоники тока, управляемый реактор, реактивная мощность.*

Библиогр.2, ил.1

УДК 004.056.5

Процедура оценки качества нейросетевого преобразователя "Биометрия - код доступа" на основе ЭЭГ / С.М. Гончаров, А.Е. Боршевников // Вестник Морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

В статье приведено сравнение характеристик нейросетевого преобразователя "Биометрия - код доступа" на основе электроэнцефалограммы с требованиями стандарта ГОСТ Р 52633.0-2006. Особое внимание уделяется вопросам расчета характеристик преобразователя: среднему расстоянию Хемминга, коэффициенту парной корреляции и стабильности выходного кода. Показано соответствие исследуемого нейросетевого преобразователя требованиям действующего стандарта в области высоконадежной биометрической аутентификации.

Ключевые слова: *биометрия, нейросетевой преобразователь "Биометрия - код доступа", электроэнцефалограмма, информационная безопасность*.

Библиогр.7, табл. 1.

УДК 004.056.5

Расширенная модель нейросетевого преобразователя "Биометрия - код доступа" на основе ЭЭГ / С.М. Гончаров, А.Е. Боршевников // Вестник Морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

В статье приведено описание расширенной математической модели нейросетевого преобразователя "Биометрия - код доступа" на основе электроэнцефалограммы. Приводится разграничение и описание входных и выходных данных модели. Описаны свойства, которым модель удовлетворяет полностью или частично. Обозначено направление дальнейшего исследования корректности описанной модели.

Ключевые слова: *биометрия, нейросетевой преобразователь "Биометрия - код доступа", электроэнцефалограмма, математическая модель, информационная безопасность*.

Библиогр.3.

УДК 004.738.2

Локализация и маршрутизация в беспроводных подводных сетях, используемых в охране мариферм / Е.В. Каменная И.А. Щербинина // Вестник Морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

В статье приведены и проанализированы методы локализации, используемые в подводных беспроводных сетях и рассмотрены традиционно используемые протоколы передачи данных.

Ключевые слова: *подводная связь, протоколы обмена, локализация, маршрутизация, латерация*.

Библиогр.5, табл.1, ил. 4

УДК 004.942

Математическая модель теплового насоса и её реализация в среде Matlab / Е. В. Касьянова // Вестник Морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

В статье приведена математическая модель теплового насоса. Описана методика реализация модели в среде Matlab/Simulink с помощью S-функции. Приведен листинг программного кода S-функции.

Ключевые слова: *моделирование, тепловой насос, S-функция*.

Библиогр.7, табл.1, ил. 1.

УДК 004.942

Обзор методов идентификации динамических объектов / Е. В. Касьянова // Вестник Морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

В статье рассмотрено состояние и основные направления теории идентификации динамических систем. Приведена классификация основных типов идентификационных моделей.

Ключевые слова: *идентификация, тепловой насос, S-функция*.

Библиогр. 4.

УДК 62-97/-98

Разработка стенда на базе микроконтроллера Arduino Mega2560 для исследования характеристик высоковольтных батареи гибридного автомобиля / С.А. Клименко // Вестник Морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

В статье приведены и проанализированы проблемы использования высоковольтных батарей для гибридного автомобиля. Приведено существующее решение задачи и предложена структура универсального стенда для реализации встроенной системы для измерения характеристик. Для реализации стенда предложено использовать микроконтроллерную систему на базе Arduino Mega2560.

Ключевые слова: *микроконтроллер, встроенная система, Arduino*

Библиогр.3, ил. 1.

УДК 62-97/-98

Обзор программируемого логического контроллера компании Овен ПЛК 110/ ПЛК 160 / С.А. Клименко // Вестник Морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

В статье приведены и проанализированы модификации программируемого логического контроллера компании Овен. Приведена сравнительная таблица характеристик контроллеров ОВЕН ПЛК110/160 и модернизированного контроллера ПЛК110[МО2].

Ключевые слова: *микроконтроллер, встроенная система, Arduino*

Библиогр.2, табл. 2.

УДК 656.61.052.65.011.56 (0.75.8)

Точность определения возвышения антенны судового приёмника GP-37 вблизи станции DGPS / Ю. А. Комаровский // Вестник Морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

В результате обработки статистического материала, полученного в ходе экспериментальных наблюдений на расстоянии 2,48 миль от дифференциальной станции мыса Поворотного, было установлено, что среднее квадратическое отклонение измеренных возвышений неподвижной антенны составило ±1,74 м. Следовательно, приближение к базовому приёмнику морской дифференциальной станции может повысить на 35% точность определения возвышений.

Ключевые слова: *GPS-приёмник, дифференциальные поправки, пространственная декорреляция, возвышение антенны, среднее квадратическое отклонение*.

Библиогр.6, табл. 1. ил. 1.

УДК 355: 528.2; 623.64

Алгоритм перехода к координатам геодезической системы ГСК-2011 / Ю. А. Комаровский // Вестник Морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

В связи с вводом в действие новой отечественной системы геодезических координат возникает необходимость иметь надёжный и точный способ пересчёта координат антенн судовых GPS-приёмников из системы WGS-84, принятой в судовождении, в координаты системы ГСК-2011. В работе обоснован и подробно описан порядок такого преобразования, основанного на способе 7 параметров Гельмерта. Предложенный алгоритм перехода может быть реализован в новых мультисистемных судовых навигационных приёмниках, а также может применяться для контроля точности преобразования координат в закупаемой аппаратуре.

Ключевые слова: *WGS-84, ГСК-2011, GPS-приёмник, способ Гельмерта, геодезическая система, преобразование координат*.

Библиогр.4, табл. 1.

УДК 656.62.052.4

Свойства горизонтального геометрического фактора судового GPS/GLONASS-приёмника SGN-500 / Ю. А. Комаровский // Вестник Морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

Оснащение судов мультисистемными спутниковыми навигационными приёмниками вызывает необходимость исследования их точности определения координат. До настоящего времени в судовой спутниковой аппаратуре в качестве показателя точности используется горизонтальный геометрический фактор. В данной работе на основе обработки экспериментального материала исследуется этот показатель, вычисляемый приёмником SGN-500. Показано, что его величины значительно отличаются от соответствующих величин, вычисляемых приёмником GP-37. Обнаружена низкая повторяемость характера суточного изменения горизонтального геометрического фактора приёмника SGN-500.

Ключевые слова: *ГГФ, HDOP, точность определения координат, судовой СРНС-приёмник, эмпирическое распределение HDOP*.

Библиогр.6, табл. 1, ил. 4.

УДК 534.2

Повышение эффективности подавления виброакустического канала утечки информации в упругих средах / В.Т. Матецкий, Д.Ю. Прощенко, А.А. Чехленок// Вестник Морского государственного университета. Сер. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

В статье приведены и проанализированы особенности распространения звуковых волн в упругих средах и рассмотрены способы повышения эффективности подавления виброакустического канала утечки информации.

Ключевые слова: *виброакустический канал, спектральная плотность сигнала, передаточная функция ограждения*

Библиогр.2, ил. 4.

УДК 004(075.8)

Антивирусная сеть / С.Н. Павликов, В.Ю. Коломеец, В.В. Динкилакер, Л.В. Степанушкин //Вестник морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

В статье предложено новое техническое решение построения сетевого экрана с использованием принципов эшелонированности, ассиметричности, управляемости, аудита и адаптации антивирусной сети, обеспечивших достижение скрытность защищаемой сети, повышенной надежности обнаружения и классификации вредоносного продукта, а также с повышенной пропускной способностью.

Ключевые слова: *вирус, антивирусная программа, сеть, эффективность.*

Библиогр. 3, табл. 1, ил. 2.

УДК 621.39

Математическая модель обеспечения безопасности объекта на море / С.Н. Павликов, Е.И. Убанкин, А.С. Цепелева, М.Д. Пленник //Вестник морского государственного университета . Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток : Мор. гос. ун-т, 2017. – Вып. 78/2017.

В статье приведена уточненная математическая модель обеспечения безопасности на море. Разработанные авторами технологии позволяют управлять качественными параметрами систем связи, повышая своевременность, достоверность и точность в широком диапазоне значений, что в итоге повышает эффективность системы обеспечения безопасности объектов на море.

Ключевые слова: *системы связи, безопасность, математическая модель, технологические решения*.

Библиогр.2, ил. 2.

УДК 004.052.2

Обзор существующих технологий применения бесконтактных карт / А.П. Патенкова, И.А. Щербинина // Вестник морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

В статье рассматриваются современные подходы к обеспечению безопасности использования бесконтактных карт и возникающие при этом риски. Особое внимание уделено протоколам обмена информации, используемым в бесконтактных технологиях и их недостаткам.

Ключевые слова: *бесконтактные карты, смарт-карты,RFID, протоколы обмена данными.*

Библиогр.6, ил. 2

УДК 004.052.2

Рейтинг профессорско-преподавательского состава как инструмент повышения эффективности работы вуза / А.Е. Пафнутьева, И.А. Щербинина //Вестник морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

В статье оценка эффективности деятельности преподавателей рассмотрена как задача теории управления сложными системами.

Ключевые слова: *оценка эффективности, рейтинг преподавателей*.

Библиогр.6, ил. 2

УДК 621.396

Развитие методов и средств доставки водолазов к месту проведения работ / С.В. Пашкеев, О.В. Пузин //Вестник морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

В статье приведен анализ задач, функций и оборудования для буксировщика водолаза, обеспечивающего подводную навигацию, безопасность плавания и свободу рук водолаза.

Ключевые слова: *водолазная техника, средства доставки водолазов, гидроакустические системы*.

Библиогр.5.

УДК 004.052.2

Существующие подходы к защите клиентской части веб-приложений / А.О. Перцев, С.Е. Путилова, И.А. Щербинина //Вестник морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

Клиентская часть современных веб-приложений постоянно усложняется. При этом механизмы защиты информации клиентской части приходится разрабатывать с оглядкой на современные и устаревшие технологии, поскольку требуется обеспечить совместимость. В статье рассмотрен подход к защите клиентской части веб-приложений на основе единого политики одинакового источника и приведены типичные приёмы обхода ограничений этого подхода.

Ключевые слова: *безопасность веб-приложений, политика одинакового источника, механизмы обеспечения безопасности клиентской части веб-приложений*.

Библиогр. 4, табл. 1.

УДК 629.12.523

Особенности динамики морского судна / К.Н. Пляшешник // Вестник Морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

В статье рассматриваются основные понятия динамики судна: качка, ходкость, управляемость, а также основные категории моделей динамики морских объектов.

Ключевые слова: *качка, ходкость, управляемость, динамика морского судна*.

Библиогр. 2.

УДК 534.014.4, 537.862

Спонтанные упруго-емкостные колебания в системах автоматики / И.П. Попов // Вестник Морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

Показано, что искусственная или упругая индуктивность электрических двигателей с упругой нагрузкой при взаимодействии с распределенными или сосредоточенными емкостными элементами цепи управления может приводить к созданию электрических колебательных контуров, в которых могут возникать свободные гармонические колебания, которые могут иметь как отрицательное, так и положительное воздействие на систему в целом.

Ключевые слова: *емкостная масса, инертная емкость, упругая индуктивность и индуктивная упругость*.

Библиогр. 10, ил. 1

УДК 621.37

Метод защиты информации в мобильных телекоммуникационных системах / А.К. Стволовая, С.Н. Павликов, Е.И. Убанкин // Вестник морского государственного университета . Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

В статье предложен метод обеспечения скрытности радиоканала, что обеспечивает защиту информации от несанкционированного получения и значительно усложняет работу оператора станции радиоразведки.

Ключевые слова: *информация, радиоканал, защита, методы, классификация*.

Библиогр.3, ил. 3.

УДК 621.37

Метод маскирования информации / Е.И Убанкин, А.К. Стволовая, С.Н. Павликов //Вестник морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

В статье предложен метод обеспечивающий маскирование, что обеспечивает защиту информации от несанкционированного доступа и усложняющий работу станции радиоразведки.

Ключевые слова: *информация, радиоканал, защита, методы, классификация, широкополосный канал*.

Библиогр.2, табл. 1, ил. 3.

УДК 531:681.5.01:629.5

Идентификация параметров нелинейной модели судна с использованием степенных рядов / Е.П. Чинчукова, Н.Ю. Поршкевич, Н.Р. Чижиков // Вестник Морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

Представлен подход идентификации параметров нелинейного объекта с неопределенными параметрами на основе метода скоростного градиента. Модель объекта управления, судна, представлена нелинейной моделью Норбина.

Ключевые слова: *адаптивное управление, робастное управление, системы с неопределенными параметрами, нелинейные модели, настройка параметров*.

Библиогр.10, ил. 14

УДК 539.19+519.2

Информационные аспекты второго закона термодинамики / А. В. Шевцов // Вестник Морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии. – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

Рассмотрено применение второго закона термодинамики на информационно неизолированные физические системы (широко известный пример «демон Максвелла»). При этом возникает иллюзия возможности осуществления вечного двигателя второго рода. Показано, что это связано с отсутствием учёта статистического взаимодействия с окружающей средой системы, измеряющей информацию о системе. Корректным является одновременное рассмотрение комплекса этой измерительной системы с физической системой (с термостатом). Для такого комплекса парадокс благополучно разрешается.

Ключевые слова: *второй закон термодинамики, количество информации и физическая энтропия, «демон Максвелла».*

Библиогр.3.

УДК 621.321

Один подход к задаче шкалирования информационных мер и метрик / А. В. Шевцов // Вестник Морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информа-ционные технологии . – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

Рассмотрен практический подход к задаче унификации и калибровки информационных мер и метрик, которые в ряде случаев удобно использовать для анализа практических результатов вместо стандартных статистических методов или совместно с ними. Именно такое параллельное применение статистических и

информационных показателей и сравнительный анализ результатов может помочь в решении этой задачи. Тестовые расчёты на практических учебных занятиях подтвердили перспективность предлагаемого подхода.

Ключевые слова: *методика оценки эффективности, статистика, коэффициент корреляции, дивергенция Кульбака, метрика Шеннона, критерий Колмогорова – Смирнова*.

Библиогр.8.

УДК 621.391

О семантических аспектах теории информации / А. В. Шевцов // Вестник Морского государственного университета. Сер. Автоматическое управление, математическое моделирование и информационные технологии . – Владивосток: Мор. гос. ун-т, 2017. – Вып. 78/2017.

Создание общей теории информации, как можно более всеобъемлющее осмысление самого понятия «информации», её роли в окружающем нас мире, по-прежнему является актуальным. В настоящее время мы имеем достаточно хорошо формализованный и разработанный вплоть до многочисленных научно-технических приложений т. н. «сигнальный» или «синтаксический» аспект этой теории. В предлагаемой работе уделено внимание состоянию дел в разработке более-менее формализованных подходов к «семантическому» осмыслению информации. Прорыв в этом направлении может перевернуть подход к культурно-эстетическому восприятию мира.

Ключевые слова: *информация, дезинформация, семиотика, семантика, актуация, тезаурус, логическая вероятность, условно-ложное предложение.*

Библиогр. 16, ил. 2

ОГЛАВЛЕНИЕ

Научное издание

Вестник Морского государственного университета

Серия: Автоматическое управление, математическое моделирование и информационные технологии

Вып. 78/2017

9. 1 уч.-изд.л. Формат 60 × 84/16

Тираж экз. Заказ №

Отпечатано в типографии ИПК МГУ им. адм. Г.И. Невельского

Владивосток 59, ул. Верхнепортовая, 50а