



Томский государственный университет систем управления и радиоэлектроники

- РАДИОТЕХНИЧЕСКИЙ
ФАКУЛЬТЕТ
- РАДИОКОНСТРУКТОРСКИЙ
ФАКУЛЬТЕТ
- ФАКУЛЬТЕТ
ЭЛЕКТРОННОЙ ТЕХНИКИ
- ФАКУЛЬТЕТ
СИСТЕМ УПРАВЛЕНИЯ
- ФАКУЛЬТЕТ
ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ
- ГУМАНИТАРНЫЙ
ФАКУЛЬТЕТ
- ФАКУЛЬТЕТ
БЕЗОПАСНОСТИ
- ЭКОНОМИЧЕСКИЙ
ФАКУЛЬТЕТ
- ФАКУЛЬТЕТ
ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ
- ЮРИДИЧЕСКИЙ
ФАКУЛЬТЕТ
- ЗАОЧНЫЙ И ВЕЧЕРНИЙ
ФАКУЛЬТЕТ
- ФАКУЛЬТЕТ
ДИСТАНЦИОННОГО
ОБУЧЕНИЯ



**ВЫБИРАЯ БУДУЩЕЕ,
ВЫБИРАЙ TUSUR!**

634050, г. Томск, пр. Ленина, 40, каб. 129 E-mail: onir@main.tusur.ru
Телефон/Факс: (3822) 900-100 Сайт: <http://tusur.ru/>

Информационный центр абитуриента: magistrant.tusur.ru

НАУЧНАЯ СЕССИЯ TUSUR–2018



**МАТЕРИАЛЫ МЕЖДУНАРОДНОЙ
НАУЧНО-ТЕХНИЧЕСКОЙ КОНФЕРЕНЦИИ
СТУДЕНТОВ, АСПИРАНТОВ
И МОЛОДЫХ УЧЕНЫХ**
16–18 мая 2018 г. (в пяти частях)

Часть 4

г. Томск

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)»

НАУЧНАЯ СЕССИЯ ТУСУР–2018

Материалы
Международной научно-технической конференции
студентов, аспирантов и молодых ученых
«Научная сессия ТУСУР–2018»

16–18 мая 2018 г., г. Томск

В пяти частях

Часть 4

В-Спектр
2018

УДК 621.37/.39+681.518 (063)

ББК 32.84я431+32.988я431

Н 34

Н 34 Научная сессия ТУСУР–2018: материалы Международной научно-технической конференции студентов, аспирантов и молодых ученых, Томск, 16–18 мая 2018 г.: в 5 частях. – Томск: В-Спектр, 2018. – Ч. 4. – 248 с.

ISBN 978-5-91191-387-8

ISBN 978-5-91191-391-5 (Ч. 4)

Материалы Международной научно-технической конференции студентов, аспирантов и молодых ученых посвящены различным аспектам разработки, исследования и практического применения радиотехнических, телевизионных и телекоммуникационных систем и устройств, сетей электро- и радиосвязи, вопросам проектирования и технологии радиоэлектронных средств, аудиовизуальной техники, бытовой радиоэлектронной аппаратуры, а также автоматизированных систем управления и проектирования. Рассматриваются проблемы электроники СВЧ- и акустооптоэлектроники, нанофотоники, физической, плазменной, квантовой, промышленной электроники, радиотехники, информационно-измерительных приборов и устройств, распределенных информационных технологий, вычислительного интеллекта, автоматизации технологических процессов, в частности, в системах управления и проектирования, информационной безопасности и защиты информации. Представлены статьи по математическому моделированию в технике, экономике и менеджменте, антикризисному управлению, правовым проблемам современной России, автоматизации управления в технике и образовании, а также работы, касающиеся социокультурных проблем современности, экологии, мониторинга окружающей среды и безопасности жизнедеятельности.

УДК 621.37/.39+681.518 (063)

ББК 32.84я431+32.988я431

ISBN 978-5-91191-387-8

ISBN 978-5-91191-391-5 (Ч. 4)

© Том. гос. ун-т систем управления
и радиоэлектроники, 2018

**Международная
научно-техническая конференция
студентов, аспирантов и молодых ученых
«Научная сессия ТУСУР–2018»,
16–18 мая 2018 г.**

ПРОГРАММНЫЙ КОМИТЕТ

- Шелупанов А.А. – председатель Программного комитета, ректор ТУСУРа, директор Института системной интеграции и безопасности, председатель правления Томского профессорского собрания, д.т.н., проф.;
- Мешеряков Р.В. – заместитель председателя Программного комитета, проректор по научной работе и инновациям ТУСУРа, зав. каф. БИС, д.т.н., проф.;
- Абдрахманова М.В., директор библиотеки ТУСУРа;
- Агеев Е.Ю., начальник научного управления, к.и.н.;
- Афонасова М.А., зав. каф. менеджмента, д.э.н., проф.;
- Бабур-Карателли Г.П.; к.т.н., PhD (TU Delft), научный сотрудник каф. ТОР ТУСУРа;
- Беляев Б.А., зав. лаб. электродинамики и СВЧ-электроники ин-та физики СО РАН, д.т.н., г. Красноярск;
- Васильковская Н.Б., доцент каф. экономики, к.э.н., доцент;
- Голиков А.М., доцент каф. РТС, к.т.н.;
- Грик Н.А., зав. каф. ИСР, д.и.н., проф.;
- Давыдова Е.М., декан ФБ, доцент каф. КИБЭВС, к.т.н.;
- Демидов А.Я., проф. каф. ТОР, к.ф.-м.н., доцент;
- Дмитриев В.М., проф. каф. КСУП, д.т.н., проф.;
- Дробот П.Н., доцент каф. УИ, к.ф.-м.н.;
- Еханин С.Г., проф. каф. КУДР, д.ф.-м.н., доцент;
- Заболоцкий А.М., проф. каф. ТУ, д.т.н.;
- Зариковская Н.В., доцент каф. ЭМИС, к.ф.-м.н., доцент;
- Исакова А.И., доцент каф. АСУ, доцент, к.т.н.;
- Карателли Д., PhD [Sapienza University of Rome], технический директор компании «The Antenna Company Nederland B.V.»;
- Карташев А.Г., проф. каф. РЭТЭМ, д.б.н., проф.;
- Катаев М.Ю., проф. каф. АСУ, д.т.н., проф.;
- Коцубинский В.П., зам. зав. каф. КСУП, доцент каф. КСУП, к.т.н., доцент;
- Красинский С.Л., декан ЮФ, к.и.н.;
- Лощилов А.Г., зав. каф. КУДР, начальник СКБ «Смена» ТУСУРа, к.т.н.;
- Лукин В.П., зав. лаб. когерентной и адаптивной оптики ИОА СО РАН, почетный член Американского оптического общества, д.ф.-м.н., проф., г. Томск;
- Малюк А.А., проф. каф. «Кибербезопасность» НИЯУ МИФИ, к.т.н., г. Москва;
- Малютин Н.Д., директор НИИ систем электрической связи, проф. каф. КУДР, д.т.н., проф.;
- Михальченко Г.Я., директор НИИ ПрЭ, д.т.н., проф.;
- Мицель А.А., проф. каф. АСУ, д.т.н., проф.;
- Мозгунов А.В., начальник ОНиР;
- Озеркин Д.В., декан РКФ, к.т.н., доцент;

- Покровская Е.М., зав. каф. ИЯ, доцент, к.филос.н.;
- Разинкин В.П., проф. каф. ТОР НГТУ, д.т.н., проф., г. Новосибирск;
- Семенов Э.В., проф. каф. РСС, д.т.н., доцент;
- Сенченко П.В., декан ФСУ, доцент каф. АОИ, к.т.н., доцент;
- Суслова Т.И., декан ГФ, зав. каф. ФиС, д.филос.н., проф.;
- Троян П.Е., зав. каф. ФЭ, проректор по учебной работе, д.т.н., проф.;
- Хаминов Д.В., зав. каф. ТП, зам. декана ЮФ, к.и.н.;
- Ходашинский И.А., проф. каф. КИБЭВС, д.т.н., проф.;
- Шарангович С.Н., проф., зав. каф. СВЧнКР, к.ф.-м.н.;
- Шостак А.С., проф. каф. КИПР, д.т.н.

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ

- Мещеряков Р.В., проректор по научной работе и инновациям ТУСУРа, зав. каф. БИС, д.т.н., проф.;
- Агеев Е.Ю., начальник научного управления, к.т.н.;
- Коротина Т.Ю., заведующая аспирантурой, к.т.н.;
- Юрченкова Е.А., вед. инженер ОППО, к.х.н.;
- Медовник А.В., председатель Совета молодых ученых, доцент каф. физики, к.т.н.;
- Боберь Ю.Н., инженер ОППО;
- Покровская Е.М., зав. каф. ИЯ, доцент, к.филос.н.

СЕКЦИИ КОНФЕРЕНЦИИ

Секция 1. Радиотехника и связь

- Подсекция 1.1. Радиотехнические системы и распространение радио-
волн. Председатель секции – *Тисленко Владимир Ильич*, проф.
каф. РТС, д.т.н.; зам. председателя – *Захаров Фёдор Николае-
вич*, доцент каф. РТС, к.т.н.
- Подсекция 1.2. Проектирование и эксплуатация радиоэлектронных
средств. Председатель секции – *Шостак Аркадий Степанович*,
проф. каф. КИПР, д.т.н.; зам. председателя – *Озёркин Денис
Витальевич*, декан РКФ, к.т.н.
- Подсекция 1.3. Радиотехника. Председатель секции – *Семенов Эдуард
Валерьевич*, проф. каф. РСС, доцент, д.т.н.; зам. председателя –
Артищев Сергей Александрович, доцент каф. КУДР, м.н.с. СКБ
«Смена», к.т.н.
- Подсекция 1.5. Аудиовизуальная техника, цифровое телерадиовеща-
ние и информационный сервис. Председатель секции – *Курячий
Михаил Иванович*, доцент каф. ТУ, к.т.н.; зам. председателя –
Костевич Анатолий Геннадьевич, доцент каф. ТУ, к.т.н., с.н.с.
- Подсекция 1.6. Инфокоммуникационные технологии и системы ши-
рокополосного беспроводного доступа. Председатель секции –
Демидов Анатолий Яковлевич, зав. каф. ТОР, к.ф.-м.н.;

зам. председателя – *Гельцер Андрей Александрович*, доцент каф. ТОР, к.т.н.

Подсекция 1.7. Робототехника. Председатель секции – *Коцубинский Владислав Петрович*, доцент каф. КСУП, к.т.н.; зам. председателя – *Винник Александр Евгеньевич*, н.с. каф. КСУП.

Подсекция 1.8. Интеллектуальные системы проектирования технических устройств. Председатель секции – *Шурыгин Юрий Алексеевич*, первый проректор, зав. каф. КСУП, д.т.н., проф.; зам. председателя – *Черкашин Михаил Владимирович*, доцент каф. КСУП, к.т.н.

Секция 2. Электроника и приборостроение

Подсекция 2.1. Проектирование биомедицинских электронных и наноэлектронных средств. Председатель секции – *Еханин Сергей Георгиевич*, проф. каф. КУДР, д.ф.-м.н. доцент; зам. председателя – *Романовский Михаил Николаевич*, доцент каф. КУДР, к.т.н.

Подсекция 2.2. Разработка контрольно-измерительной аппаратуры. Председатель секции – *Лоцилов Антон Геннадьевич*, зав. каф. КУДР, начальник СКБ «Смена», к.т.н.; зам. председателя – *Убайчин Антон Викторович*, с.н.с. СКБ «Смена», к.т.н.

Подсекция 2.3. Физическая и плазменная электроника. Председатель секции – *Троян Павел Ефимович*, проректор по УР, зав. каф. ФЭ, д.т.н., проф.; зам. председателя – *Смирнов Серафим Всеволодович*, проф. каф. ФЭ, д.т.н.

Подсекция 2.4. Промышленная электроника. Председатель секции – *Михальченко Геннадий Яковлевич*, директор НИИ ПрЭ, д.т.н., проф.; зам. председателя – *Семёнов Валерий Дмитриевич*, проф. каф. ПрЭ, к.т.н.

Подсекция 2.5. Оптические информационные технологии, нанофотоника и оптоэлектроника. Председатель секции – *Шарангович Сергей Николаевич*, проф., зав. каф. СВЧиКР, к.ф.-м.н.; зам. председателя – *Перин Антон Сергеевич*, доцент каф. СВЧиКР, к.т.н.

Подсекция 2.6. Электромагнитная совместимость. Председатель секции – *Заболоцкий Александр Михайлович*, проф. каф. ТУ, д.т.н.; зам. председателя – *Куксенко Сергей Петрович*, доцент каф. ТУ, к.т.н.

Подсекция 2.7. Светодиоды и светотехнические устройства. Председатель секции – *Туев Василий Иванович*, зав. каф. РЭТЭМ, д.т.н.; зам. председателя – *Вилисов Анатолий Александрович*, проф. каф. РЭТЭМ, д.т.н.

Секция 3. Информационные технологии и системы

- Подсекция 3.1. Интегрированные информационно-управляющие системы. Председатель секции – *Катаев Михаил Юрьевич*, проф. каф. АСУ, д.т.н.; зам. председателя – *Суханов Александр Яковлевич*, доцент каф. АСУ, к.т.н.
- Подсекция 3.2. Распределённые информационные технологии и системы. Председатель секции – *Сенченко Павел Васильевич*, декан ФСУ, доцент каф. АОИ, к.т.н.; зам. председателя – *Сидоров Анатолий Анатольевич*, доцент каф. АОИ, к.т.н.
- Подсекция 3.3. Автоматизация управления в технике и образовании. Председатель секции – *Дмитриев Вячеслав Михайлович*, проф. каф. КСУП, д.т.н.; зам. председателя – *Ганджа Тарас Викторович*, доцент каф. КСУП, к.т.н.
- Подсекция 3.4. Моделирование в естественных и технических науках. Председатель секции – *Зариковская Наталья Вячеславовна*, доцент каф. ЭМИС, к.ф.-м.н.; зам. председателя – *Колотаев Илья Владимирович*, разработчик ООО «СибирьСофтПроект».
- Подсекция 3.5. Вычислительный интеллект. Председатель секции – *Ходашинский Илья Александрович*, проф. каф. КИБЭВС, д.т.н.; зам. председателя – *Сарин Константин Сергеевич*, доцент каф. КИБЭВС, к.т.н.
- Подсекция 3.6. Современные библиотечные технологии. Председатель секции – *Абдрахманова Марина Викторовна*, директор библиотеки ТУСУРа; зам. председателя – *Карауш Александр Сергеевич*, доцент каф. РСС, к.т.н.
- Подсекция 3.7. Молодежные инновационные научные и научно-технические проекты. Председатель секции – *Дробот Павел Николаевич*, доцент каф. УИ, к.ф.-м.н.; зам. председателя – *Нариманова Гуфана Нурлабековна*, зав. каф. УИ, к.ф.-м.н., доцент.
- Подсекция 3.8. Разработка программного обеспечения. Председатель секции – *Гордиевских Вячеслав Валерьевич*, генеральный директор ООО «СибирьСофтПроект»; зам. председателя – *Зариковская Наталья Вячеславовна*, доцент каф. ЭМИС, к.ф.-м.н.
- Подсекция 3.9. Инструментальные средства поддержки автоматизированного проектирования и управления. Председатель секции – *Хабибулина Надежда Юрьевна*, доцент каф. КСУП, к.т.н.; зам. председателя – *Потапова Евгения Андреевна*, ст. преподаватель каф. КСУП.

Секция 4. Информационная безопасность

- Подсекция 4.1. Методы и системы защиты информации. Информационная безопасность. Председатель секции – *Шелупанов Алек-*

сандр Александрович, ректор ТУСУРа, директор ИСИБ, д.т.н., проф.; зам. председателя – *Конев Антон Александрович*, доцент каф. КИБЭВС, к.т.н.

Подсекция 4.2. Радиоэлектронные системы передачи информации и средства их защиты. Председатель секции – *Голиков Александр Михайлович*, доцент каф. РТС, к.т.н.; зам. председателя – *Бернгардт Александр Самуилович*, доцент каф. РТС, к.т.н.

Подсекция 4.3. Экономическая безопасность. Председатель секции – *Кузьмина Елена Александровна*, доцент каф. КИБЭВС, к.т.н.; зам. председателя – *Глухарева Светлана Владимировна*, ст. преподаватель каф. КИБЭВС.

Секция 5. Экономика, управление, социальные и правовые проблемы современности

Подсекция 5.1. Моделирование в экономике. Председатель секции – *Мицель Артур Александрович*, проф. каф. АСУ, д.т.н.; зам. председателя – *Грибанова Екатерина Борисовна*, доцент каф. АСУ, к.т.н.

Подсекция 5.2. Информационные системы в экономике. Председатель секции – *Исакова Анна Ивановна*, доцент каф. АСУ, к.т.н.; зам. председателя – *Григорьева Марина Викторовна*, доцент каф. АСУ, к.т.н.

Подсекция 5.3. Современные методы финансового планирования. Председатель секции – *Васильковская Наталья Борисовна*, доцент каф. экономики, к.э.н.; зам. председателя – *Цибулькикова Валерия Юрьевна*, доцент каф. экономики, к.э.н.

Подсекция 5.4. Проектный менеджмент и его использование в цифровой экономике. Председатель секции – *Афонасова Маргарита Алексеевна*, зав. каф. менеджмента, д.э.н.; зам. председателя – *Богомолова Алена Владимировна*, декан ЭФ, доцент каф. менеджмента, к.э.н.

Подсекция 5.5. Современные социокультурные технологии в организации работы с молодежью. Председатель секции – *Суслова Татьяна Ивановна*, декан ГФ, зав. каф. ФиС, д.филос.н., проф.; зам. председателя – *Орлова Вера Вениаминовна*, проф. каф. ФиС, директор НОЦ «СГТ», д.соц.н.

Подсекция 5.6. Актуальные проблемы социальной работы в современном обществе. Председатель секции – *Грик Николай Антонович*, зав. каф. ИСР, д.и.н., проф.; зам. председателя – *Куренков Артем Валериевич*, доцент каф. ИСР, к.и.н.

Школа-семинар: Правовые проблемы современной России. Председатель секции – *Хаминов Дмитрий Викторович*, зав. каф. ТП, зам. декана ЮФ, к.и.н.; зам. председателя – *Газизов Родион Маратович*, ст. преподаватель каф. ИП.

Секция 6. Экология и мониторинг окружающей среды. Безопасность жизнедеятельности. Председатель секции – *Карташев Александр Георгиевич*, проф. каф. РЭТЭМ, д.б.н.; зам. председателя – *Денисова Татьяна Владимировна*, доцент каф. РЭТЭМ, к.б.н.

Секция 7. Открытия. Творчество. Проекты. (Секция для школьников). Председатель секции – *Мозгунов Алексей Викторович*, начальник ОНиР; зам. председателя – *Колесник Анастасия Викторовна*, инженер ОНиР.

Секция 8. Postgraduate and Master Students' Research in Electronics and Control Systems. (Секция на английском языке). Председатель секции – *Покровская Елена Михайловна*, зав. каф. ИЯ, доцент, к.филос.н.; зам. председателя – *Шпит Елена Ирismetовна*, ст. преподаватель каф. ИЯ; *Соболевская Ольга Владимировна*, ст. преподаватель каф. ИЯ.

Круглый стол. Интеграция образовательных технологий и ресурсов школы, техникума и вуза в целях повышения качества непрерывной подготовки специалистов.

Адрес оргкомитета:

**634050, Россия, г. Томск, пр. Ленина, 40,
ФГБОУ ВО «ТУСУР», научное управление (НУ), к. 205
Тел.: 8-(382-2) 701-524; e-mail: nstusur@main.tusur.ru**

Распределение публикаций по секциям и частям сборника:

1-я часть – 1-я секция (подсекции 1.1 – 1.8);

2-я часть – 2-я секция (подсекции 2.1 – 2.7);

3-я часть – 3-я секция (подсекции 3.1 – 3.9);

4-я часть – 4-я секция (подсекции 4.1 – 4.3);

6-я секция; 8-я секция; доклады круглого стола;

5-я часть – 5-я секция (подсекции 5.1 – 5.6); школа-семинар.

7-я секция – доклады школьников печатаются отдельным сборником.

Спонсор конференции – Группа компаний «Научное оборудование»



Группа компаний	383 330 8295
«Научное оборудование»	495 150 3295
630128, Россия, г. Новосибирск,	www.spegroup.ru
ул. Инженерная, 4а, оф. 212	

Группа компаний «Научное оборудование» была образована в 1999 г. Основное направление деятельности компании – снабжение высокотехнологичным оборудованием учебных, научно-исследовательских и промышленных предприятий Сибири и Дальнего Востока России.

Мы анализируем задачи заказчика, подбираем оборудование под каждый конкретный случай, осуществляем поставку оборудования, а также оказываем технологическую и методологическую поддержку, гарантийный и послегарантийный ремонт. Некоторые наши заказчики доверяют нам полное закрытие всех потребностей своих лабораторий и в оборудовании, и в расходных материалах.

В штате компании состоят высококвалифицированные технические специалисты с собственным опытом научной работы. Наши специалисты регулярно знакомятся с новинками оборудования, с новыми подходами в приборостроении, посещают международные выставки и обучающие семинары от производителей. Для каждой задачи заказчика мы можем предложить самое современное решение. Существующие рабочие связи со многими лабораториями СО РАН позволяют оперативно привлекать к решению задач заказчика профильных научных специалистов. Кроме того, мы сами организуем мастер-классы и семинары, на которых наши заказчики имеют уникальную возможность познакомиться с новейшим оборудованием для решения своих задач.

У нас налажены партнерские отношения со многими ведущими мировыми производителями научного и технологического оборудования как в России, так и за рубежом. У компании есть свой инженерный департамент; в случае необходимости мы можем самостоятельно разработать решение непосредственно под задачу заказчика.

Нашими заказчиками являются все академические институты Сибирского отделения Российской академии наук, многие промышленные предприятия, технологические компании, учебные заведения высшего образования Сибирского и Дальневосточного регионов.

Кроме деятельности по поставке и разработке оборудования, мы участвуем в продвижении разработок институтов СО РАН на внешний рынок, организуем совместные проекты институтов СО РАН с разными организациями по разработке конкретных технологических и наукоёмких решений.

Мы видим своей целью построение долгосрочных взаимовыгодных отношений с каждым нашим заказчиком.

Спонсор конференции – ООО «Кейсайт Текнолоджиз»



ООО «Кейсайт Текнолоджиз»
Россия, 115054, г. Москва
Космодамианская наб., 52, стр. 3

Тел.: 495 797 39 00
Факс: 495 797 39 02
www.keysight.ru

Keysight Technologies – мировой технологический лидер на рынке контрольно-измерительных решений для электронной, оборонной, аэрокосмической и телекоммуникационной промышленности.

Как самостоятельная компания Keysight Technologies была образована в 2014 г. в результате стратегического разделения компании Agilent Technologies, которая, в свою очередь, до 1999 г. входила в корпорацию Hewlett-Packard. Первый измерительный прибор под маркой Hewlett-Packard был выпущен более 75 лет назад.

В настоящий момент компания Keysight Technologies предоставляет самый широкий на рынке спектр лабораторных, модульных и портативных контрольно-измерительных приборов, в т.ч. оборудование для радиоизмерений (генераторы сигналов, анализаторы сигналов, анализаторы цепей), осциллографы и приборы общего назначения (мультиметры, источники питания, генераторы импульсов, системы сбора данных, логические анализаторы, ручные приборы), решения для тестирования телекоммуникаций, а также системы автоматизированного проектирования и моделирования электронных устройств.

В России приборы Keysight Technologies, ранее производимые под маркой Hewlett-Packard/Agilent, используются уже более 45 лет и по праву считаются наиболее точным и надежным контрольно-измерительным оборудованием на рынке.

Российский офис компании Keysight Technologies предлагает своим клиентам локальную техническую и сервисную поддержку, техническую документацию на русском языке. Для серий малогабаритных осциллографов, генераторов сигналов и анализаторов спектра разработаны русскоязычные интерфейсы пользователя. На большинство приборов есть сертификаты об утверждении типа средств измерений. На постоянной основе ведется работа по включению в Госреестр новых приборов Keysight Technologies.

Среди крупнейших заказчиков Keysight Technologies в России ведущие научно-исследовательские институты, конструкторские бюро, вузы, крупнейшие операторы связи.

В 2012 г. компания Keysight Technologies открыла два дополнительных региональных офиса в России – в Приволжском и Сибирском федеральных округах. В 2013 г. дополнительный офис открыт в Ростове-на-Дону, в 2014 г. – в Санкт-Петербурге.

Информация о компании Keysight Technologies доступна в сети Интернет по адресу: www.keysight.ru

Генеральный директор ООО «Кейсайт Текнолоджиз»

Смирнова Галина Владимировна

СЕКЦИЯ 4

**ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ**

ПОДСЕКЦИЯ 4.1

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

*Председатель секции – Шелупанов А.А., ректор ТУСУРа,
директор ИСИБ, д.т.н., проф.;*
зам. председателя – Конев А.А., доцент каф. КИБЭВС, к.т.н.

НАПИСАНИЕ ПРАВИЛ НОРМАЛИЗАЦИИ И КОРРЕЛЯЦИИ ДЛЯ ВЫЯВЛЕНИЯ СЛЕДОВ АРТ ПРИ ПОМОЩИ MAXPATROL SIEM

Т.С. Косаченко, М.А. Андреев, студенты
*Научный руководитель А.И. Гуляев, ассистент;
А.А. Конев, доцент, к.т.н.; Д.С. Никифоров, аспирант
г. Томск, ТУСУР, каф. КИБЭВС, gai@keva.tusur.ru,
kaa1@keva.tusur.ru, hds@csp.tusur.ru
Проект ГПО КИБЭВС–1711 «Методы и алгоритмы
для определения сетевых атак»*

Изначально под АРТ (advanced packaging tool) взломом подразумевались кибернападения на военные организации, однако в настоящее время они не ограничены только военной сферой. Данный вид угроз широко распространен в крупных коммерческих организациях. Основная угроза заключена в том, что атака сконцентрирована на одной цели, которой может стать конкретная компания или государственная организация.

Кибератака делится на несколько этапов, некоторые из которых могут длиться в течении месяцев или даже лет. Каждое действие оставляет следы в системе, которые будут использоваться для исследования является ли данное событие инцидентом информационной безопасности (ИБ).

Для этой задачи использовался MaxPatrol SIEM – система выявления инцидентов ИБ. Для его работы необходимо предоставить события в нормализованном виде (используя правила нормализации) и правила корреляции (для описания зависимостей между событиями для признания их инцидентом). Сбор событий осуществлял Kaspersky

Endpoint Security 10. Все программное обеспечение было развернуто в виртуальной машине Windows Server 2012.

Особый интерес в событиях вызывали следующие поля:

- код события;
- время создания;
- название объекта;
- путь к объекту.

Пример части нормализованного события представлен на рис. 1.

```
norm {  
  "mime": "text/csv",  
  "category.low": "Detection",  
  "subject": "application",  
  "id": "Kaspersky_ODBC_GNRL_EV_VIRUS_FOUND",  
  "event_src.vendor": "kaspersky",  
  "tag": "odbclog",  
  "event_src.category": "Host security",  
  "object": "malware",  
  "subject.version": "10.2.2.10535",  
  "object.type": "60",  
  "event_src.hostname": "7X64-FORENSIC",  
  "_nks": [["10.10.10.30"], ["7X64-FORENSIC"], ["10.10.9.9"]],  
  "taxonomy_version": "0.1.232-master",  
  "event_src.title": "security_center",  
  "object.path": "C:\\Users\\username\\Desktop\\leicar\\leicar.com",  
  "object.name": "EICAR-Test-File",  
  "event_src.ip": "10.10.10.30",  
  "category.high": "Miscellaneous",  
  "generator": "N9.1.169",  
  "action": "detect",
```

Рис. 1. Нормализованное событие

Для установления, является ли определенное событие инцидентом, необходимо его унифицировать с помощью написанных правил нормализации. В таком виде MaxPatrol SIEM способен находить между событиями взаимосвязи, для этой цели были написаны правила корреляции. Результатом вышеперечисленных действий станет однозначный ответ: является ли данное событие интересующим нас инцидентом.

Написание дополнительных правил нормализации и корреляции необходимо, так как не существует универсальных, полностью удовлетворяющих нашей ситуации, а именно поиску следов АРТ. Чтобы написать правило корреляции, необходимо знать последовательность событий, которые составляют инцидент. Каждое правило включает в себя: условие, глубину выборки, исключения и сценарий.

После чтения каждого события модуль корреляции принимает одно из следующих решений:

- событие не соответствует ни одному правилу;
- если правило срабатывает после наступления одного или нескольких событий, создается экземпляр корреляции и обновляется счетчик;
- при срабатывании всех условий, инцидент регистрируется.

В ходе группового проектного обучения были написаны правила нормализации и корреляции для MaxPatrol SIEM, позволяющие объединить последовательность составных событий в логическую сущность и генерировать факт проникновения в систему. Корректность работы была проверена с помощью программного обеспечения для разработки MaxPatrol SIEM.

ЛИТЕРАТУРА

1. Мониторинг событий и управление инцидентами ИБ [Электронный ресурс]. – Режим доступа: <http://www.acti.ru/resheniya-i-uslugi/informatcionnaia-bezopasnost/bezopasnostit-infrastruktury/monitoring-sobyti-i-upravlenie-incidentami-ib/> (дата обращения: 26.02.18).
2. MAXPATROL SIEM 14.0. Руководство оператора. – ЗАО «Позитив Технолоджиз», 2016.
3. Kaspersky Endpoint Security 10 Service Pack 2 для Windows. Организация защиты компьютера [Электронный ресурс]. – Режим доступа: <https://help.kaspersky.com/keswin/10sp2/ru-ru/127971.htm> (дата обращения: 28.02.18).
4. Kaspersky Endpoint Security 10 Service Pack 2 для Windows. Аппаратные и программные требования [Электронный ресурс]. – Режим доступа: <https://help.kaspersky.com/keswin/10sp2/ru-ru/127972.htm> (дата обращения: 01.03.18).

СОВРЕМЕННЫЕ ПОДХОДЫ К СНИЖЕНИЮ ПОКАЗАТЕЛЯ СИГНАЛ-ШУМ В КАНАЛЕ УТЕЧКИ ПЭМИ

Д.А. Антипов, аспирант

Научный руководитель А.А. Шелупанов, д.т.н., проф., зав. каф. КИБЭВС г. Томск, ТУСУР, каф. КИБЭВС, antipodp@gmail.com, rector@tusur.ru

Основной показатель, по которому оценивается защищённость информации от утечки по каналу побочного электромагнитного излучения (ПЭМИ) является соотношение сигнал/шум. Чем больше это соотношение, тем проще выделить информативный сигнал из смеси сигнал+шум. Источником информативного сигнала выступает любое функционирующее электронное устройство. Из-за физики распространения электромагнитных волн, в пространство вокруг устройства

неизбежно проникает побочное излучение, несущее в себе информативный сигнал.



Рис. 1. Функциональная схема канала утечки ПЭМИ

Традиционно, существует два способа снижения соотношения сигнал/шум. Первый – это снижение уровня излучаемой мощности сигнала, второй – повышение уровня шума. При этом считается, что если в окружающую обстановку не привнесено новой энергии, такой способ называется пассивным. Если же устройство защиты информации само излучает какие-либо сигналы, этот способ называется активным. Иначе можно классифицировать эти способы так: если у устройства нет отдельного питания, его можно считать пассивным; если оно есть – активным. Также популярно третье понимание этого разделения: если снижается уровень излучаемого сигнала – это пассивное средство защиты, если повышается уровень шума – это активное средство защиты.

Целью данной работы является анализ актуальных исследований, посвященных способам снижения показателя сигнал/шум. Эти подходы тоже будем разбивать на две категории: активные и пассивные. Хотя целью этих работ не ставится снижение показателя сигнал/шум, в конечном счете, результаты работ подразумевают повышение защищённости информации, что количественно можно оценить в этом показателе.

Активные подходы. Так как самым популярным средством активной защиты является генератор электромагнитного шума, большая часть исследований направлена на оптимизацию его характеристик.

- Расширение спектра излучения, для перекрытия устройств, работающих на частотах выше 3 ГГц.
- Обеспечение избирательности зашумления, что оставляет возможность функционирования гражданским устройствам [1–3].
- Использование шума с характеристиками, которые подобны характеристикам сигнала, что делает информативный сигнал невозможным [4–7].
- Использование информации о направленности излучения и подстройка работы ГЭШ.

Пассивные методы. Пассивные методы можно разделить на две группы: программные и технические. Программным методам посвящено большое количество исследований, в которых говорится, что особая работа с отображаемой информацией позволяет существенно снизить уровень ПЭМИ.

- Алгоритм хаотичного вывода информации на монитор делает информативный сигнал не обрабатываемым статистическими методами.
- Использование одного из трёх цветовых каналов RGB, при этом генерируя шум на остальных двух каналах, снижает уровень излучения.
- Использование особых шрифтов делает излучаемый сигнал менее выразительным из-за пониженной контрастности и резкости переходов от светлых участков текста к тёмным. [8]
- Хаотичный доступ к файлам жесткого диска делает перехват ПЭМИ безрезультативным.
- Применение экранирующих тканей в дополнение к ГЭШ позволяет исключить перехват ПЭМИ частотах выше 1 ГГц. [9]

Выводы

1. Современные подходы к пассивным мерам позволяют значительно снизить уровень ПЭМИ.
2. Существует множество методов оптимизации шума от ГЭШ, однако присутствует недостаток технических реализаций этих подходов.

ЛИТЕРАТУРА

1. Урбанович П.В., Югов Н.Т., Шелупанов А.А. Средство формирования шумовой электромагнитной помехи // Научный вестник Новосиб. гос. техн. ун-та. – 2012. – С. 121–126.
2. Шелупанов А.А., Югов Н.Т., Урбанович П.В. Определение режимов для формирования полос частот средств активной защиты // Доклады ТУСУРа. – 2010. – Вып. № 1 (21), ч. 1. – С. 78–81.
3. Урбанович П.В. Генератор шума с подстройкой диапазонов // Доклады ТУСУРа. – 2008. – Вып. № 2 (18), ч. 1. – С. 9–11.
4. Егин А.В., Святкин С.А., Паршуткин А.В. Применение структурных и шумовых помех для защиты информации от утечки по каналу побочных электромагнитных излучений // Вопросы оборонной техники. Сер. 16: Технические средства противодействия терроризму. – 2016. – С. 27–34.
5. Землянухин П.А. Многоканальный адаптивный генератор шума для маскирования ПЭМИН // Известия ЮФУ. Технические науки. – Сентябрь 2016. – С. 82–93.
6. Петров И.С. Оценка энергетической эффективности метода формирования маскирующих помех путём записи/воспроизведения сигналов ПЭМИ от СВТ // Технологический институт Федерального государственного образо-

вательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге. – Вып. 14. – 2010. – С. 171–175.

7. Богаченков К.Н., Маслаков П.А. Вознюк В.В. Особенности создания помех компенсационного типа для решения задач защиты информации от утечки по техническим каналам // Труды военно-космической академии им. А.Ф. Можайского. – 2015. – Вып. 646. – С. 83–92.

8. Мищенко Д.А. Железнов Д.И. Защита информации от утечки через побочные электромагнитные излучения видеосистемы компьютера // Научно-практический электронный журнал «Аллея Науки». – 2017. – Вып. 10.

9. Петигин А.Ф. Применение радиоэкранирующих тканей для защиты информации от утечки за счёт побочных электромагнитных излучений // REDS: Телекоммуникационные устройства и системы. – 2015. – №5. – Вып. 4. – С. 428–431.

ПРОГРАММНО-АППАРАТНЫЕ КОМПЛЕКСЫ «БЛОКХОСТ»

А.Е. Гуськов, А.И. Дзангиев, М.А. Першин, студенты

Научный руководитель А.Ю. Якимук, м.н.с. каф. КИБЭВС

г. Томск, ТУСУР, aguskov1995@gmail.com

*«Проект ГПО КИБЭВС-1704 «Средства защиты
операционных систем»*

В настоящее время стремительный рост компьютеризации глобально изменил образ жизни людей. Одновременно с проникновением технологий в человеческую жизнь недостаточная защищенность компьютерных систем от несанкционированного доступа повышает риск возникновения нештатных ситуаций, способных вызвать непредсказуемые последствия, от финансовых потерь, до техногенных катастроф [1].

Эту проблему решают различные системы защиты информации (СЗИ) от несанкционированного доступа (НСД). Так как в сферу компетенции специалистов направления «Информационной безопасности» входит установка, настройка и обслуживание средств защиты информации, возникла идея рассмотреть средства защиты информации, которые не включены в программу обучения, на предмет того, какие полезные функции они содержат.

Нами были рассмотрены три программно-аппаратных комплекса (ПАК) по обеспечению защиты от несанкционированного доступа (НСД) – «Блокхост-МДЗ», «Блокхост-Сеть К» и «Блокхост-ЭЦП».

Программно-аппаратный комплекс (ПАК) «Блокхост-МДЗ» предназначен для предотвращения несанкционированного доступа к ресурсам вычислительной техники на начальном этапе загрузки.

Главные достоинства программы – шифрование разделов жесткого диска, в том числе системного, и внешних носителей. При шифровании можно использовать такие носители ключевой информации, как eToken и RuToken [2].

Функционал системы шифрования поможет студентам получить навыки работы с реальными системами шифрования, используемые в организациях и государственных структурах, и подготовит к работе в различных организациях.

ПАК «Блокхост-ЭЦП» предназначен для защиты электронного документооборота.

Главное достоинство программы – управление электронно-цифровой подписью. Поддержка иностранных криптосистем дает возможность обмениваться электронными документами с зарубежными организациями [3].

Это позволит студентам ознакомиться с системами защищенного электронного документооборота.

ПАК «Блокхост-сеть К» предназначен для защиты информации на автоматизированных системах обрабатывающих конфиденциальную информацию.

Его главное достоинство – контроль и разграничение к запуску процессов, а также встроенный персональный сетевой экран. Контроль запуска обеспечивает надежную защиту от посторонних процессов в операционной системе, а сетевой экран предотвращает сетевые атаки [4].

При работе с этой программой студент закрепит знания в системном администрировании, сетевых технологиях защиты данных и освоит контроль над процессами.

Все представленные программы обладают таким дополнительным функционалом, как отслеживание целостности файлов, очистка памяти, контроль подключаемых устройств. Дополнительно ПАК «Блокхост-МДЗ» и «Блокхост-сеть К» контролируют идентификацию и аутентификацию пользователей с использованием хранилищ ключевой информации и не дают загрузиться системе, если таковые не предоставлены.

В ходе работы с программами студент может закрепить навыки, полученные при изучении таких предметов, как «Основы информационной безопасности», «Организация ЭВМ и вычислительных систем», «Безопасность операционных систем», «Криптографические методы защиты информации», «Управление средствами защиты информации», «Системное администрирование», «Программно-аппаратные средства защиты информации» [5].

Невысокие технические требования программного комплекса позволяют студентам использовать для обучения техническое обеспечение университета.

ЛИТЕРАТУРА

1. Иванько А.Ф., Иванько М.А., Шанина А.А. Информационная безопасность вчера и сегодня // Молодой ученый. – 2017. – №51. – С. 25–30.
2. ГазИнформСервис – Описание применения ПАК Блокхост-МДЗ [Электронный ресурс]. – Режим доступа: <http://www.gaz-is.ru/component/jdownloads/send/7-mdz/6-opisanie-primeneniya-bh-mdz.html> (дата обращения: 03.03.2018).
3. ГазИнформСервис – Описание применения ПАК Блокхост-МДЗ [Электронный ресурс]. – Режим доступа: <http://www.gaz-is.ru/component/jdownloads/send/16-2013-11-07-14-39-42/151-litoria-desktop-manual-install.html> (дата обращения: 07.03.2018).
4. Руководство пользователя средства защиты информации от несанкционированного доступа «Блокхост-Сеть К» // ГазИнформСервис. – 2013 – С. 3–20.
5. ТУСУР – 10.03.01 Информационная безопасность [Электронный ресурс]. – Режим доступа: <https://edu.tusur.ru/programs/731> (дата обращения: 01.03.2018).

ПРИМЕНЕНИЕ ЗНАКОВЫХ ГРАФОВ И ТЕОРИИ СТРУКТУРНОГО БАЛАНСА ДЛЯ ПОСТРОЕНИЯ МОДЕЛИ ИНФОРМАЦИОННОЙ ВОЙНЫ

*А.А. Бедарева, А.А. Колесникова, М.А. Куртова, студентки
Научные руководители Е.М. Давыдова, доцент каф. КИБЭВС, к.т.н.;
А.А. Шелупанов зав. каф. КИБЭВС, д.т.н.
г. Томск, ТУСУР, каф. БИС, dem@keva.tusur.ru
Проект ГПО КИБЭВС–1713 «Информационная война
против России»*

Задачи, приводящие к знаковым графам, возникли впервые в социологии при изучении проблемы сбалансированности малых групп, т.е. того, насколько группа, состоящая из нескольких участников, может эффективно работать.

Предположим, что следует составить группу из трех человек и необходимо спрогнозировать, насколько без конфликтов будет работать эта группа. Можно предполагать, что бесконфликтная работа будет обеспечена, если отношения между членами группы хорошие. Эти отношения могут быть описаны в терминах «симпатия-антипатия», «дружба-неприязнь» и т.п., т.е. отношения между членами группы описываются бинарными отношениями, а если говорить о работе

группы без конфликтов, необходимо найти уже какую-то интегральную характеристику, касающуюся группы в целом. Такой характеристикой является мера сбалансированности соответствующего знакового графа.

К исследованию сбалансированности сводятся также некоторые задачи политического анализа, исследования сложных систем разного рода. Например, понятие баланса можно применить к анализу отношений среди стран, участвующих в конфликте с Россией.

Введем в рассмотрение граф, вершины которого соответствуют членам группы. Для краткости они будут называться участниками или индивидуумами. Дуги между вершинами a и b отмечаются знаком «+», если участник a симпатизирует участнику b , и знаком «-», если между ними существуют неприязненные отношения. Если же a и b равнодушны друг к другу, дуга между соответствующими вершинами отсутствует. Такой граф называется знаковым [1].

Рассмотрим все возможные типы ситуаций, которые характеризуют отношения между членами группы из трех человек. Они показаны на рис. 1.

Можно заметить, что группы на рис. 1, a и $в$ сбалансированы, а группы на рис. 1, $б$ и $г$ – нет.

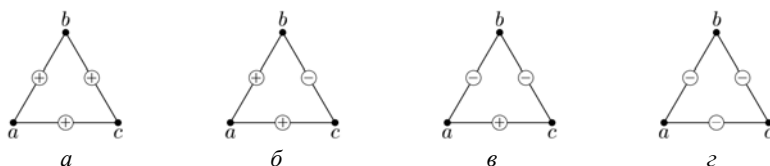


Рис. 1. Отношения между членами группы из трех человек

В соответствующем знаковом графе вершины можно разделить на два подмножества таким образом, что любая дуга, соединяющая вершины из одного множества, имеет знак «+», а дуги, соединяющие вершины из разных подмножеств – знак «-».

Для сравнения сбалансированности графов необходимо для каждого знакового графа определить меру сбалансированности, соответствующую «относительному» балансу графа, так чтобы у более сбалансированных графов была выше мера сбалансированности.

Обозначим через C^+ число положительных циклов в графе G , а через C – число всех простых циклов. Тогда мера сбалансированности G определяется как

$$b(G) = C^+ / C. \quad (1)$$

Рассмотрим, как можно применить знаковые графы к анализу информационной войны против России. Если вершины графа изобра-

жают некоторые страны, то мера сбалансированности может быть определена по формуле (1). Здесь, однако следует сказать несколько слов о вычислительной сложности алгоритмов.

Из самого определения сбалансированности ясно, что необходимо проверить все простые циклы графа G . Будем считать, что наш граф полный, то есть все страны находятся между собой в некоторых отношениях, хороших или плохих. Тогда его простые циклы соответствуют подмножествам множества N , кроме подмножеств, содержащих 2 элемента. Таким образом, для того чтобы найти все подмножества графа G и рассчитать, являются ли соответствующие циклы положительными, необходимо проделать не менее 2^n операций, где n – число вершин графа. Как известно, в мире 251 страна, т.е. полное исследование сбалансированности отношений между отдельными странами не представляется возможным. Поэтому, будем рассматривать постановку задачи, в которой вершинами графа G будут основные участники в информационной войне против России. Список участников, включая Россию представлен в табл. 1.

Граф для модели этой информационной войны представлен на рис. 2.

Рис. 2. Граф для модели информационной войны: Р – Россия, С.Е – страны Евросоюза, Г – Грузия

Таблица 1
Список основных участников в информационной войне

Название
США
Россия
Страны Евросоюза
Грузия

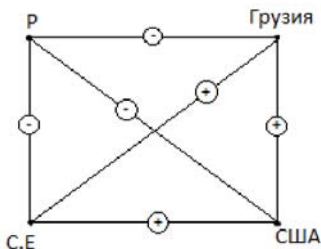


Таблица 2
Циклы графа

Цикл	Знак
С.Е-Р-Г-С.Е	–
С.Е-Р-США-С.Е	–
С.Е-Г-США-С.Е	–
Р-Г-США-Р	–
С.Е-Р-Г-США-С.Е	+
С.Е-Р-США-Г-С.Е	+
С.Е-Г-Р-США-С.Е	+

На данном графе можно увидеть, что все страны имеют «отрицательные» отношения к России, но между США, Грузией и странами Евросоюза существует «положительные» отношения.

Рассмотрим граф на рис. 2 и подсчитаем для него меру сбалансированности. В первом столбце табл. 2 выписаны все простые циклы графа, во втором стоит «+» или «–» в зависимости от знака цикла.

Здесь $b(G) = C^+ / C = 3/7$.

Из данных расчетов делаем вывод, что система несбалансированная.

Можно сделать вывод, что знаковые графы применимы во многих сферах нашей жизни. В том числе их можно применять для составления моделей информационных войн.

ЛИТЕРАТУРА

1. Лекция № 3. Знаковые графы и теория структурного баланса [Электронный ресурс]. – URL: <https://studfiles.net/preview/3350247>

2. Теория структурного баланса Фрица Хайдера [Электронный ресурс]. – URL: <http://www.psychologyrise.ru/pris-349-1.html>

ОСНОВНЫЕ УГРОЗЫ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ И МЕТОДЫ ЗАЩИТЫ ОТ НИХ

Ф.И. Кропачев, Д.А. Мех, А.А. Исанов, студенты

г. Томск, ТУСУР, каф. КСУП, uncle.thed@gmail.com

Появление виртуализации привело к переходу большинства систем на виртуальные машины, однако решение задач обеспечения безопасности, связанных с эксплуатацией приложений в новой среде, требует особого подхода. Многие типы угроз достаточно изучены [1], и для них разработаны средства защиты, однако их еще нужно адаптировать для использования в облаке [2].

В основе обеспечения физической безопасности лежит строгий контроль физического доступа к серверам и сетевой инфраструктуре. В отличие от физической безопасности, сетевая безопасность в первую очередь представляет собой построение надежной модели угроз, включающей в себя защиту от вторжений и межсетевой экран. Использование межсетевого экрана подразумевает работу фильтра с целью разграничить внутренние сети ЦОД на подсети с разным уровнем доверия. Это могут быть отдельно серверы, доступные из Интернета, или серверы из внутренних сетей.

Рассмотрим список 12 угроз облачной безопасности [3], представленный организацией SCA (Cloud Security Alliance) на конференции RSA в 2016 г.

1. Утечка данных. Облачные провайдеры обычно развертывают средства безопасности для защиты своих окружений, но в конечном итоге организации несут ответственность за защиту своих собственных данных в облаке. Для предотвращения утечек информации, многие компании используют технологию DLP, позволяющую в автома-

тическом режиме организовывать проверку информационных потоков, обнаруживать в них конфиденциальные данные, и в итоге применять к ним определенные действия. Рекомендуется использовать многофакторную аутентификацию и шифрование.

2. Компрометация учетных записей и обход аутентификации.

Данные могут быть скомпрометированы в результате физической потери носителя, передачи информации по незащищенным каналам в незашифрованном виде, несанкционированного доступа постороннего лица, перехвата информации вредоносными программами, прослушивания каналов связи, сознательной передачи носителя с данными третьему лицу. Многофакторные системы аутентификации, такие как одноразовые пароли, аутентификация на основе телефона и смарт-карты, защищают облачные сервисы, поскольку они затрудняют вход в систему с украденными паролями.

3. Взлом интерфейсов и API. API и интерфейсы, как правило, являются наиболее уязвимой частью системы, потому что они обычно доступны из открытого Интернета. CSA рекомендует организовать адекватный контроль доступа, использовать инструменты защиты и раннего обнаружения угроз. Также рекомендуется выполнять проверку безопасности кода и запускать тесты на проникновение.

4. Уязвимость используемых систем. Системные уязвимости и вредоносные ошибки в программах стали более серьезной проблемой с появлением многоуровневости в облачных вычислениях. Однако атаки на уязвимости системы можно смягчить ITIL процессами, расходы на внедрение которых малы по сравнению с потенциальным ущербом.

5. Кража учетных записей. Необходимо запретить совместное использование учетных данных между пользователями и службами, а также обратить внимание на механизмы многофакторной аутентификации. Сервисные аккаунты и учетные записи пользователей необходимо контролировать, детально отслеживая выполняемые транзакции.

6. Инсайдеры-злоумышленники. В облачном сценарии инсайдер способен уничтожить целые инфраструктуры или манипулировать данными. Системы, которые зависят исключительно от поставщика облачных услуг для обеспечения безопасности, таких как шифрование, подвергаются наибольшему риску. В качестве защиты необходимо контролировать процесс шифрования. А также не стоит забывать про логирование, мониторинг и аудит событий по отдельно взятым учетным записям.

7. Целевые кибератаки. Злоумышленника, задавшегося целью установить и закрепить собственное присутствие в целевой инфра-

структуре, не так легко обнаружить. Для минимизации рисков и профилактики подобных угроз поставщики облачных услуг используют продвинутое средства безопасности. Но помимо использования современных решений, рекомендуется проводить специализированное обучение сотрудников по распознаванию техник злоумышленника.

8. Перманентная потеря данных. Несмотря на то, что случаи потери данных без возможности восстановления по причине поставщика услуг стали крайне редкими, злоумышленники постоянно удаляют облачные данные, чтобы нанести вред предприятиям. Облачные поставщики рекомендуют отделять пользовательские данные от данных приложений, сохраняя их в различных локациях. Необходимы адекватные меры резервного копирования данных, а также соблюдение передовой практики непрерывности бизнеса и аварийного восстановления.

9. Недостаточная осведомленность. Операционные и архитектурные проблемы возникают, если команде разработчиков компании не хватает знания облачных технологий, поскольку приложения развертываются в конкретном облаке. Рекомендуется тщательно ознакомиться с технологией, чтобы учесть риски, при использовании любой облачной службы.

10. Злоупотребление облачными сервисами. Облачные сервисы могут быть задействованы для поддержки несанкционированных действий, таких как запуск DDoS-атак, отправку спама и фишинговых писем. Провайдером необходимо распознавать типы злоупотреблений и предлагать инструменты клиентам для мониторинга состояния среды их облака. Несмотря на то, что клиенты могут не быть прямой добычей для вредоносных действий, злоупотребление облачным сервисом может по-прежнему приводить к проблемам доступности услуг и сбоям данных.

11. DDoS-атаки. В результате DoS-атак может сильно замедлиться или вовсе прекратиться работа значимых для бизнеса компании сервисов. Несмотря на то, что облачные провайдеры, как правило, лучше ориентированы на DoS-атаки, чем их клиенты, необходимо иметь план смягчения атаки до того, как она произойдет.

12. Совместные технологии. Уязвимости в общих технологиях создают значительную угрозу для облачных вычислений. Если встроенный компонент получает компрометацию он потенциально подвергает риску. CSA рекомендует всестороннюю стратегию защиты, включая многофакторную аутентификацию на всех хостах, системы обнаружения вторжений на основе хоста и сети, применяя концепцию наименьших привилегий, сегментацию сети и исправление общих ресурсов.

Многие проблемы, связанные с защитой виртуализации, требуют тщательного анализа и проработанного решения, поэтому наиболее правильный и эффективный способ минимизировать риски безопасности – на основе сделанного прогноза разработать политику безопасности, отвечающую интересам собственника, и в соответствии с ней построить систему безопасности.

ЛИТЕРАТУРА

1. Бердник А.В., Бойко А. Методы защиты виртуальной среды // Всероссийский журнал научных публикаций. – 2013. – № 3 (18). – С. 24–27.
2. Угрозы облачных вычислений и методы их защиты [Электронный ресурс]. – URL: <https://digdes.ru/press/5259> (дата обращения: 12.03.2018).
3. The top 12 cloud security threats [Электронный ресурс]. – URL: <https://www.networkworld.com/article/3042610/security/the-dirty-dozen-12-cloud-security-threats.html> (дата обращения: 12.03.2018).

ОБЗОР ПОДХОДОВ К ВЫБОРУ НАИЛУЧШЕГО ИЗОБРАЖЕНИЯ-КОНТЕЙНЕРА ДЛЯ СТЕГАНОГРАФИЧЕСКОГО ВСТРАИВАНИЯ ИНФОРМАЦИИ

А.С. Кокурина, В.С. Мельман, инженеры

*Научный руководитель О.О. Евсютин, доцент каф. БИС, к.т.н.
г. Томск, ТУСУР, каф. БИС и КИБЭВС, annakokurina94@yandex.ru*

Методы стеганографического встраивания информации в цифровые изображения должны обеспечивать достижение таких характеристик как незаметность, высокая ёмкость и устойчивость перед стегоанализом. Существует большое количество способов повышения этих важных показателей качества встраивания. Одним из них является выбор наиболее подходящего для встраивания стегоконтейнера. Целью настоящей работы является обзор и анализ существующих подходов к выбору наилучшего контейнера.

Авторы работы [1] предлагают поиск наилучшего контейнера для встраивания секретного изображения на основе векторов признаков изображений. Учитываются такие статистические признаки как среднее, дисперсия, асимметрия, а также информация о соседних пикселях. Для встраивания выбирается изображение, содержащее больше всего блоков, похожих на блоки секретного изображения. Для кластеризации векторов признаков контейнера используется алгоритм К-средних. Евклидово расстояние применяется для измерения близости блоков контейнера и блоков секретного изображения.

В работе [2] встраивание информации осуществляется в область дискретного вейвлет-преобразования. Для повышения качества

встраивания авторы предлагают использовать выбор наилучшего контейнера на основе расчёта корреляции между битами секретного сообщения и младшими битами поддиапазонов HH, HL и LH. Для встраивания используется изображение, у которого самая высокая корреляция с информацией, которую нужно скрыть в данном изображении. Согласно результатам экспериментов, данный подход на 10% уменьшает число изменений на этапе встраивания.

Работа [3] показывает, что правильный выбор контейнера в формате JPEG способен значительно повысить устойчивость к стегоанализу. В работе все характеристики, которые должны учитываться при выборе контейнера, делятся на два класса. К первому классу относятся характеристики, связанные только с оригинальным изображением-контейнером: это число изменяемых коэффициентов дискретного косинусного преобразования (ДКП) и качество JPEG-сжатия. Ко второму классу относятся характеристики, связанные одновременно с контейнером и соответствующим стегоизображением, например, число изменений коэффициентов ДКП, метрики MSE и SSIM.

В статье [4] выбор контейнера дополняет метод встраивания информации в коэффициенты контурного преобразования. Авторы делят характеристики, влияющие на пригодность изображения для встраивания, на две категории. К быстрым оценкам относятся такие, которые могут быть вычислены единожды для последующего быстрого к ним обращения. Эта категория связана с определением сложности и текстурности изображения. К точным оценкам относятся такие, которые рассчитываются с учётом секретного сообщения. В эту категорию входит визуальное качество, оцениваемое метрикой PSNR, и количество изменений, которые необходимо выполнить во время встраивания информации.

Авторы [5] также осуществляют встраивание в область контурного преобразования. Из базы изображений для встраивания выбираются изображения с высоким значением контрастности, поскольку они обеспечивают наибольшую ёмкость встраивания.

В [6] предлагается схема, направленная на повышение устойчивости к стегоанализу за счёт выбора наилучшего контейнера и его предварительной обработки. В качестве меры для выбора контейнера используются такие характеристики как контрастность, яркость и темнота. Требуется оценка функции распределения вероятности контейнера и стегоизображения, для чего используется классификатор, основанный на методе опорных векторов. Из базы изображений выбираются такие, чьи функции распределения вероятности незначительно изменялись после встраивания.

В работе [7] выбор контейнера зависит от задаваемого пользователем параметра, определяющего требуемый уровень безопасности. В первую очередь определяется, достаточна ли ёмкость изображения для сокрытия сообщения, а затем происходит расчёт, сравнение результатов которого с параметром позволяет определить, подходит ли изображение для встраивания.

Обобщая вышеизложенное, можно отметить, что описанные подходы к выбору наилучшего контейнера делятся на два класса: требует ли выбор встраивания сообщения или нет. К первому классу относятся подходы, описанные в [3, 4, 6], остальные – ко второму. Как показано в рассмотренных работах, учёт секретного сообщения позволяет добиться большей эффективности встраивания, однако требует значительных временных затрат в случае, если анализируемая база изображений достаточно велика. Однако эта проблема может быть актуальна и для первого класса подходов. Например, в [2] применение выбора контейнера увеличивает процесс встраивания 65 тысяч битов с 4,5 с до 350 мин.

Также существенно отличается количество и набор признаков, по которым осуществляется выбор контейнера. В большинстве работ выбор сводится к сортировке вариантов по какому-то одному признаку, что даёт быстрый результат. Только в работах [1, 6] учитываются одновременно несколько характеристик изображения, что делает указанные подходы более точными и гибкими, но и увеличивает время обработки базы изображений.

Различаются и цели применения выбора контейнера. В большинстве работ целью является повышение устойчивости перед стегоанализом. В работах [1, 4] также говорится об увеличении ёмкости встраивания, в [5] – только об увеличении ёмкости. В [2] идёт речь об уменьшении числа изменений при встраивании, что должно положительно сказываться на визуальном качестве стегоизображений.

Таким образом, выбор подходящего контейнера является распространённым методом повышения эффективности встраивания информации. Существует большое количество подходов к выбору, основанных на различных характеристиках анализируемых изображений и предназначенных для различных целей, таких как повышение визуального качества, ёмкости или устойчивости к стегоанализу. Однако анализ существующих подходов не выявил некоторого универсального, поэтому поиск новых таких подходов является перспективным направлением исследования.

ЛИТЕРАТУРА

1. Sajedi H., Jamzad M. Cover Selection Steganography Method Based on Similarity of Image Blocks // Proceedings of the IEEE 8th International Conference on Computer and Information Technology Workshops, 8–11 July 2008. – Australia, Sydney. – 2008. – P. 379–384.
2. Hajduk V., Levický D. Cover Selection Steganography // Proceedings of 2016 International Symposium ELMAR, 12–14 Sept. – 2016. – Croatia, Zadar. – 2016. – P. 205–208.
3. Kharrazi M., Sencar H.T., Memon N. Cover Selection for Steganographic Embedding // Proceedings of 2006 IEEE International Conference on Image Processing, 8–11 Oct. 2006. – USA, Atlanta. – 2006. – P. 117–120.
4. Sajedi H., Jamzad M. Using contourlet transform and cover selection for secure steganography // International Journal of Information Security. – 2010. – Vol. 9, №5. – P. 337–352.
5. Subhedar M.S., Mankar V.H. Performance Evaluation of Image Steganography based on Cover Selection and Contourlet Transform // Proceedings of 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies (CUBE), 15–16 Nov. – 2013. – India, Pune. – 2013. – P. 172–177.
6. Sajedi H., Jamzad M. BSS: Boosted steganography scheme with cover image preprocessing // Expert Systems with Applications. – 2010. – Vol. 37. – P. 7703–7710.
7. Sattar I.A., Gaata M.T. Image Steganography Technique based on Adaptive Random Key Generator With Suitable Cover Selection // Proceedings of 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), 7–9 March 2017. Iraq, Baghdad. – 2017. – P. 208–212.

РАЗРАБОТКА КУРСА ПРАКТИЧЕСКИХ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ «БЕЗОПАСНОСТЬ СЕТЕЙ ЭВМ»

П.В. Перминов, П.А. Ковчунов, студенты

*Научный руководитель А.К. Новохрестов, аспирант каф. КИБЭВС
г. Томск, ТУСУР, каф. КИБЭВС, perminovpetr.ppv@gmail.com*

В настоящее время с широким распространением электронно-вычислительной техники и постепенным переходом к информационному постиндустриальному обществу становится крайне актуальной профессия, в чьей сфере профессиональной деятельности лежит обеспечение информационной безопасности сетей и систем передачи информации. [1]

Согласно рабочей программе 10.05.03 – Информационная безопасность автоматизированных систем [2], после освоения учебной дисциплины «Безопасность сетей ЭВМ», студент должен овладеть следующими компетенциями:

– ПК-3 способностью проводить анализ защищенности автоматизированных систем;

- ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
- ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации;
- ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы;

Ввиду вышесказанных требований, а также постепенного устаревания уже существующих методических пособий [3], были поставлены задачи разработки курса практических и лабораторных работ по дисциплине «БСЭВМ».

В рамках поставленных задач был разработан план создания методических пособий и виртуальных машин в отдельности для каждой из следующих тем:

1. Ознакомление с работой ОС Linux, настройка протокола SSH.
2. Тестирование уровня безопасности WiFi-сети с помощью пакета утилит Aircrack-NG.
3. Тестирование уровня безопасности систем баз данных с помощью утилиты Sqlmap.
4. Анализ защищенности сайтов с помощью программного средства OWASP ZAP.
5. Работа с анализатором сетевого трафика Wireshark.
6. Тестирование на проникновение сетевой инфраструктуры с использованием фреймворка Metasploit.
7. Установка и первоначальное конфигурирование сетевой операционной системы ИКС Lite на базе FreeBSD.
8. Работа с веб-интерфейсом и менеджером отчетов сетевой операционной системы ИКС Lite.
9. Настройка и использование системы обнаружения вторжений Suricata IDS.

Соответствие работ компетенциям

Номер работы	Компетенция
1	ПК-26
2	ПК-3, ПК-14, ПК-17
3	ПК-3, ПК-14
4	ПК-3, ПК-14, ПК-17
5	ПК-17, ПК-26
6	ПК-3, ПК-17
7	ПК-26
8	ПК-17, ПК-26
9	ПК-3, ПК-17, ПК-26

В настоящее время выполнена работа по пп. 1, 2, 7.

При создании каждая работа из курса проходит стадии анализа предметной области, разработки методического пособия, тестирования на предмет соответствия техническому заданию и фактическим задачам курса, а также дорабатывается по итогам тестирования при необходимости. Данные выше три комплекта заданий для практических работ успешно протестированы и признаны релевантными.

Обобщая все вышесказанное, можно заключить, что в ходе прохождения разрабатываемого курса, вкупе с уже разработанными материалами и пособиями [4] студент должен получить:

- знания и навыки по применению защищенных протоколов передачи данных и управления, настройке локальных сетей, конфигурированию и использованию межсетевых экранов и средств обнаружения вторжений для защиты информации в сетях;
- навыки противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с требованиями нормативно правовых актов и нормативных методических документов;
- навыки анализа сетевого трафика [5].

ЛИТЕРАТУРА

1. Буренин А.Н., Легков К.Е. Вопросы безопасности инфокоммуникационных систем и сетей специального назначения: основные угрозы, способы и средства обеспечения комплексной безопасности сетей. – 2015. – 16 с. [Электронный ресурс]. – <https://cyberleninka.ru/article/v/voprosy-bezopasnosti-infokommunikatsionnyh-sistem-i-setey-spetsialnogo-naznacheniya-osnovnye-ugrozy-sposoby-i-sredstva-obespecheniya>
2. Безопасность сетей ЭВМ: рабочая программа учебной дисциплины, направление подготовки 10.05.03 – Информационная безопасность, профиль «Безопасность автоматизированных систем»: ТУСУР, 2017. – 2 с. [Электронный ресурс] – https://edu.tusur.ru/work_programs/15408
3. Новохрестов А. К., Праскурин Г.А. Безопасность сетей ЭВМ: метод. указ. для лаб. и практ. работ. – 2014. – 99 с. [Электронный ресурс]. – http://kibevs.tusur.ru/sites/default/files/upload/work_progs/nak/BSEVM_lab_pract.pdf
4. Новохрестов А.К., Праскурин Г.А. Безопасность сетей ЭВМ: метод. указ. для самостоят. работы студента. – 2014. – 4 с. [Электронный ресурс]. – http://kibevs.tusur.ru/sites/default/files/upload/work_progs/nak/BSEVM_sam.pdf
5. Праскурин Г.А. Безопасность вычислительных систем: метод. указ. по выполнению курсовой работы. – 2012. – 3 с. [Электронный ресурс]. – http://kibevs.tusur.ru/sites/default/files/upload/work_progs/nak/BVS_kurs.pdf

РАЗГРАНИЧЕНИЕ ДОСТУПА К ИНФОРМАЦИИ В СИСТЕМЕ MOODLE

А.Я. Бомбов, А.С. Репкин, А.В. Кравцова, студенты

Научный руководитель Д.В. Кручинин, н.с. каф. КИБЭВС, к.ф.-м.н.

г. Томск, ТУСУР, kruchinindm@gmail.com

Проект КИБЭВС-1701

Модульная объектно-ориентированная динамическая обучающая система – MOODLE (Modular Object-Oriented Dynamic Learning Environment), распространяющаяся свободно. Она позволяет преподавателям создавать свои собственные онлайн – курсы, проверять знания учащихся по пройденному материалу, а студентам приступать к обучению в любое время и в любом месте. Курс – пространство на сайте Moodle, где преподаватели могут добавлять учебные материалы по своим предметам для студентов [1].

Как любое другое свободно распространяющееся программное обеспечение, Moodle имеет как преимущества, так и недостатки: основным достоинством является то, что каждый может разобраться в механизме создания и редактирования заданий, а затем разместить разработанные задания в общедоступные источники информации. Но с другой стороны, это же является и главным недостатком бесплатного ПО – любой человек может получить размещенные разработки и присвоить их, вплоть до дальнейшей продажи интеллектуальной собственности.

Так как в Moodle можно экспортировать не только задания, но и целые курсы, при распространении в общедоступных источниках информации разработок, созданных в Moodle, возникает опасность плагиата или частичного копирования. Поэтому необходимо реализовать механизм, при котором создатель курса (заданий) сможет распространять свою разработку и контролировать все пути, по которым происходит ее распространение.

Для решения поставленной проблемы предлагается использование встроенного в Moodle механизма создания ролей пользователей для разработки специальной роли, обеспечивающей безопасность авторского права.

Роли пользователей. Изначально, при установке Moodle, имеется только пользователь Администратор с соответствующей ролью. Он имеет все права доступа, может создавать, удалять и редактировать задания, курсы, добавлять и изменять права пользователей, настройки безопасности сайта. При создании нового пользователя администратору предлагается выдать ему роль. Изначально представлены 8 ролей:

- менеджер;
- создатель курсов;
- преподаватель;
- преподаватель без права редактирования;
- студент;
- гость;
- аутентифицированный пользователь;
- аутентифицированный пользователь на главной странице.

Так как последние трое не имеют почти никаких прав и используются как вспомогательные, в данной работе они рассматриваться не будут.

Менеджер может предоставлять доступ к курсам и вносить исправления в них, но он обычно не является членом курсов.

Создатель курсов разрабатывает курсы.

Преподаватели имеют полные права внутри курсов, например, оценивание студентов, создание и редактирование заданий и т.д.

Преподаватели без права редактирования не могут редактировать и перемещать вопросы, добавлять новые.

Студент имеет минимальные права в курсе, обычно только на доступ и добавление информации [2].

Ни одна из этих ролей не обеспечивает полную защиту интеллектуальной собственности. Поэтому предлагается создать новую роль со следующим набором настроек (рис. 1)

Course		
Add new questions moodle/question:add	☒ Allow	 
Edit all questions moodle/question:editall	☐ Allow	 
Edit your own questions moodle/question:editmine	☒ Allow	 
<u>Flag questions while attempting them</u> moodle/question:flag	☒ Allow	
Edit question categories moodle/question:managecategory	☒ Allow	 
Move all questions moodle/question:moveall	☐ Allow	
Move your own questions moodle/question:movemine	☒ Allow	
Use all questions moodle/question:useall	☒ Allow	
Use your own questions moodle/question:usemine	☒ Allow	
View all questions moodle/question:viewall	☐ Allow	
View your own questions moodle/question:viewmine	☒ Allow	

Activity: Forum

Рис. 1. Параметры безопасности создаваемой роли

Далее приведены описание параметров:

- добавить новый вопрос. Позволяет создавать новый вопрос, импортировать вопрос и добавлять вопрос в категорию;
- править все вопросы/ свои вопросы. Позволяет изменять и удалять свои/ чьи-либо вопросы;
- маркировать вопросы при редактировании. После сохранения вопроса в поле «последнее изменение» будет фамилия изменяющего;
- изменять категории. Позволяет создавать, перемещать и менять категории вопросов;
- перемещать все вопросы/ свои вопросы. Позволяет перемещать из категории в категорию свои/чьи-либо вопросы;
- использовать все вопросы/ свои вопросы. Позволяет предварительно просматривать и использовать в тестах свои/чьи-либо вопросы;
- просматривать все вопросы/ свои вопросы. Позволяет просматривать содержимое вопроса, сохранять его как новый вопрос и импортировать в категорию;
- заданные таким образом настройки, позволяют роли просматривать созданные другим пользователем задания, но не открывать и редактировать их. На собственные вопросы пользователя – обладателя роли – разграничение не распространяется, он имеет на них полные права.

Результаты. Введение разработанной роли в систему Moodle (например заказчика электронных курсов), позволит разработчикам курсов распространять свои разработки без риска дальнейшего потери интеллектуальной собственности.

Выводы. Введение новой роли обеспечит защиту интеллектуальной собственности, что, в свою очередь, позволит разработчикам принимать заказы на разработку курсов и заданий в пределах своей организации и не беспокоиться о причинении ущерба интеллектуальной собственности.

ЛИТЕРАТУРА

1. Moodle documentation [Электронный ресурс]. – URL: https://docs.moodle.org/33/en/Main_page (дата обращения: 15.10.2017).
2. Пособие-путеводитель по документации Moodle 2.5: для начинающих [Электронный ресурс]. – URL: <http://vital.lib.tsu.ru/vital/access/manager/Repository/vtls:000480490> (дата обращения: 4.03.2018).
3. Moodle Docs 3.4 [Электронный ресурс]. – URL: https://docs.moodle.org/34/en/Main_page (дата обращения: 4.03.2018).

ЗАЩИТА ИНФОРМАЦИИ В ОПЕРАЦИОННЫХ СИСТЕМАХ СЕМЕЙСТВА LINUX

А.А. Михайлова, студент

Руководитель проекта А.Ю. Якимук, м.н.с. каф. КИБЭВС

г. Томск, ТУСУР, каф. КИБЭВС, 725_maa@fb.tusur.ru

Проект ГПО КИБЭВС–1704 «Средства защиты операционных систем»

Обеспечение безопасной и эффективной работы является актуальным вопросом как для обычных пользователей, так и для любой коммерческой или государственной организации. Современные операционные системы (ОС) обладают мощными встроенными средствами обеспечения безопасности, которые осуществляют аутентификацию, авторизацию, аудит действий пользователей в системе, защиту от сбоев, криптографическую защиту объектов операционной системы, предотвращение сетевых атак.

В ходе учебного процесса на факультете безопасности студенты изучают такой предмет, как «Безопасность операционных систем» на примере ОС Windows. С целью расширить объем знаний и умений обучающихся по данной дисциплине, была поставлена задача рассмотреть ОС Linux, а также сформировать новые лабораторные работы, позволяющие применить полученные знания на практике.

Linux является универсальной платформой, применяемой в самых различных решениях. Подсистема драйверов поддерживает динамически загружаемые модули без потерь в производительности, обеспечивая модульность (в дополнение к повышенной динамичности и переносимости платформы). Кроме того, Linux обладает защитой на уровне ядра, обеспечивающей защищенность платформы. Linux поддерживает наибольшее количество файловых систем любых ОС, что дает гибкость, обеспечиваемую модульным принципом проектирования. В Linux реализованы не только стандартные возможности планирования загрузки процессора, но и диспетчеризация в реальном времени (включая гарантированные задержки обработки прерываний). Открытость Linux минимизирует возможность внедрения вредоносного кода, повышая, таким образом, ее безопасность [1].

Благодаря возможностям трансформации и масштабирования Linux, ее можно встретить во всех областях компьютерной техники (например, десктопы и нетбуки, серверы, кластеры, мэйнфреймы, суперкомпьютеры, портативные и планшетные устройства).

Исходя из этого, можно сделать вывод, что системе безопасности в ОС семейства Linux отводится очень большое внимание.

В ходе работы рассматриваются встроенные средства обеспечения безопасности ОС Linux.

В операционной системе Linux используется простая модель доступа, основанная на субъект-субъектной модели. В современных версиях Linux помимо общей схемы можно использовать списки доступа. При этом реализуется статическая авторизация множественного доступа к объекту.

Организация парольной политики чрезвычайно важна для защиты пользователя, рабочей станции и сети, поскольку пароль является основным способом определения подлинности пользователя. Учетные данные и пароли в большинстве *nix хранятся в таких файлах, как /etc/passwd, /etc/shadow, /etc/master.passwd. Эти файлы относятся лишь к стандартной аутентификации, которая легко может быть изменена. Такие программы, как login, su, passwd, в современных системах сами не работают с паролями, а делают запрос к PAM, которая осуществляет всю процедуру аутентификации. Таким образом для обеспечения безопасности и настройки пароля используется pam_cracklib из состава Linux-PAM, который используется почти всеми современными Linux [2].

В Linux имеется множество средств для криптографической защиты информации – от шифрования почтовых переписок до шифрования файлов и блочных устройств. Шифрование на уровне файловых систем предполагает наличие прослойки между основной файловой системой и пользователем.

Шифрование блочных устройств происходит на более низком уровне, под файловой системой. При этом сама файловая система не знает, что она находится на зашифрованном томе [3].

Изучение встроенных в операционные системы семейства Linux средств, направленных на обеспечение безопасности, может быть полезным для будущих специалистов по защите информации.

Одним из наиболее подходящих для реализации данной идеи вариантом является дисциплина «Безопасность операционных систем». В рамках данного предмета лабораторные работы, в ходе которых изучаются встроенные механизмы защиты ОС семейства Linux, позволяют более углубленно освоить профессиональные компетенции. Таким образом, будет получен комплекс лабораторных, включающий такие работы как «Разграничение доступа и парольная политика», «Шифрование на уровне файловых систем» и «Аудит безопасности».

ЛИТЕРАТУРА

1. IBM developerWorks Россия: Технические материалы [Электронный ресурс]. – Режим доступа: <https://www.ibm.com/developerworks/ru/library/linuxuniversal/index.html> (дата обращения: 02.03.2018).

2. Security – парольная политика в Linux [Электронный ресурс]. – Режим доступа: <http://welinux.ru/post/3793/> (дата обращения: 05.03.2018).

3. Cryptoworld – практическая безопасность [Электронный ресурс]. – Режим доступа: <https://cryptoworld.su/шифрование-данных-в-linux/> (дата обращения: 05.03.2018)

МЕТОДИКА ОПИСАНИЯ ЗАЩИЩАЕМЫХ РЕСУРСОВ, ИСПОЛЬЗУЕМЫХ ПЕРСОНАЛОМ

Н.В. Петров, студент

Научный руководитель А.А. Конев, доцент каф. КИБЭВС, к.т.н.

г. Томск, ТУСУР, каф. БИС, nikitayahoo1995@gmail.com

В настоящее время сильно развиты и продолжают развиваться информационные технологии, что влечет за собой усиление мер по информационной безопасности. Следовательно, из этого, усиление мер по информационной безопасности требует дополнительных средств и вложений в данную область.

Прежде чем проводить модернизацию или полную замену систем по обеспечению информационной безопасности, необходимо провести проверку текущего состояния информационной безопасности компании в соответствии с определенными критериями и показателями безопасности. Для этих целей существует аудит информационной безопасности.

Этап сбора информации аудита является наиболее сложным и длительным. Это связано в основном с отсутствием необходимой документации на информационную систему и с необходимостью плотного взаимодействия аудитора со многими должностными лицами организации [3].

На данный момент существуют множество стандартов и законов, описывающих аудит информационной безопасности, но отсутствует полностью нормативно методическая документация процедурного плана по аудиту информационной безопасности.

Целью работы является разработка методики защищаемых ресурсов, используемых персоналом.

На основе анализа существующих методик по сбору информации о персонале и возможной информации, к которой необходимо применять функцию защиты [1, 2], а также ГОСТов, связанных с информационной безопасностью и аудитом [4–6] была разработана методика и разработана формализованная модель методики с использованием методологии IDEF0 с последующей декомпозицией, которая представлена на рис. 1.



Рис. 1. Модель черного ящика методики

Методика состоит из 3 этапов.

Этап первый содержит в себе следующие пункты:

1. Определение типовых ролей или эталона системы менеджмента информационной безопасности (СМИБ). Непосредственное определение типовых ролей, производится с высшим руководителем организации, либо с начальником службы информационной безопасности. Поэтому разделение на типовые роли без учета специфики организации имеет нецелесообразный характер.

2. Определение привилегий [2]. Непосредственное определение привилегий, должно производится с высшим руководителем организации, либо с начальником службы информационной безопасности.

Необходимо, чтобы в многопользовательских системах, которые требуют защиты от неавторизованного доступа, предоставление привилегий контролировалось посредством формализованного процесса авторизации [2, 3];

3. Определение источников информации [1]. Информацию о типовых ролях и о привилегиях сотрудников получаем у лиц, отвечающих за это напрямую и косвенным образом;

4. Формирование эталонной таблицы – типовая роль/привилегии.

Этап второй содержит в себе следующие пункты:

- 1) сбор фактической информации. Проверяющие должны получать фактическую информацию путем выполнения процедур по сбору;

- 2) составление фактической таблицы – типовая роль/привилегии;
- 3) сравнительный анализ с заранее заданными критериями, обговоренными с руководством организации.

Этап третий содержит в себе следующие пункты:

- 1) сопоставление таблицы из первого этапа с таблицей фактических данных из второго этапа, на соответствие или расхождение [2, 6].
- 2) оценка полученных данных;
- 3) получение результата сравнительного анализа и написание рекомендаций. На основе анализа собранного дополнительного материала определяются характер, значимость и причины выявленных проблем и соответствующим образом отражаются в выводах по результатам сравнительного анализа.

В результате была разработана методика процедурного плана, которая позволит облегчить процесс сбора информации и аудита в целом, а также поможет избежать ошибок при проведении аудиторской деятельности.

ЛИТЕРАТУРА

1. ГОСТ Р ИСО 19011–2012. Руководящие указания по аудиту систем менеджмента [Электронный ресурс]. – Режим доступа: <http://docs.cntd.ru/document/1200095049> (дата обращения: 25.12.2016);
2. ГОСТ Р ИСО/МЭК 27001–2006 Информационная технология. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности [Электронный ресурс]. – Режим доступа: <http://docs.cntd.ru/document/1200058325> (дата обращения: 25.12.2016);
3. ГОСТ Р ИСО/МЭК 27002–2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности [Электронный ресурс]. – Режим доступа: <http://docs.cntd.ru/document/1200103619> (дата обращения: 25.12.2016);
4. ГОСТ Р ИСО/МЭК 27003–2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности [Электронный ресурс]. – Режим доступа: <http://docs.cntd.ru/document/1200103165> (дата обращения: 25.12.2016);
5. ГОСТ Р ИСО/МЭК 27007–2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности [Электронный ресурс]. – Режим доступа: <http://docs.cntd.ru/document/1200112881> (дата обращения 25.12.2016);
6. NIST SP800–115. Техническое руководство по проверке и оценке ИБ. («Technical Guide to Information Security Testing and Assessment» NIST Special Publication 800–115) [Электронный ресурс]. – Режим доступа: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800–115.pdf> (дата обращения: 25.12.2016).

СИСТЕМА АУТЕНТИФИКАЦИИ ОБЪЕКТОВ ПРОМЫШЛЕННОЙ СЕТИ

Р.П. Попадинец, студент каф. КИБЭВС

*Научный руководитель А. А. Конев, доцент каф. КИБЭВС, к.т.н.
г. Томск, ТУСУР, popadinets.r@mail.ru*

В настоящее время активно развивается такое направление в области информационных технологий, как Интернет вещей (IoT, Internet of Things), представляющее совокупность разнообразных приборов, датчиков, устройств, объединённых в сеть посредством любых доступных каналов связи, использующих различные протоколы взаимодействия между собой и единственный протокол доступа к глобальной сети. В роли глобальной сети для интернет-вещей используется сеть Интернет. Общим протоколом является IP. Промышленная сеть все больше интегрируется в потребительскую сферу, автоматизированные системы управления технологическими процессами (АСУ ТП) активно используются в энергетике, например, устройства учёта, устройство сбора и передачи данных, всё это относится к автоматизированной системе коммерческого учета электроэнергии (АСКУЭ).

По статистике 2017 г., сделанной компанией Positive Technologies, [1] на первом месте, по использованию уязвимостей компонентов АСУ ТП, находится распределенные системы управления/человеко-машинный интерфейс – 31%, на втором месте сетевое устройство АСУ ТП – 28%. Процедура аутентификации устройства в сети по-прежнему остается одной из проблем в информационной безопасности. Устройства в сети Интернет, в рамках одной сети, должны проходить идентификацию и аутентификацию на управляющем сервере, отправляя свои данные как напрямую, так и через ретрансляторы, где ретрансляторами могут быть любые устройства, датчики. В момент аутентифицирования устройства, злоумышленник может подменить устройство, выдав новое устройство за подлинное или вывести его из строя. Чтобы предотвратить, или снизить ущерб от действий злоумышленника, нужно использовать надёжный протокол аутентификации.

Протоколы сетевой аутентификации. Существует несколько различных протоколов, описывающих процесс аутентификации устройств в локальной сети и при удалённом доступе с использованием открытых каналов связи – Интернет. В локальной сети используются протоколы LAN Manager, NT LAN Manager, NT LAN Manager версии 2 и Kerberos [2]. Последний протокол широко используется в операционных системах Windows и Unix, и используется последняя версия

Kerberos 5, которая была принята в качестве стандарта IETF. Для удалённого доступа можно привести в качестве примера протоколы PAP, CHAP, EAP, RADIUS, TACACS, TACACS+ и др.

Протокол Kerberos 5 основывается на выдаче субъектам так называемых «билетов» (tickets) [3] и обладает рядом преимуществ: более эффективная аутентификация на серверах за счет проверки удостоверения клиента; верификация сервера и клиента, и их взаимная аутентификация; делегированная аутентификация; упрощенное управление; совместимость со всеми сетями, где поддерживается протокол Kerberos 5. Но обладает и рядом недостатков: протокол не способен отражать атаки типа «отказ в обслуживании», «распознавание пароля»; в случае кражи ключей, злоумышленник способен выступить в роли участника сессии или в роли какого-либо сервера для другого законного участника сессии.

Протокол RADIUS описан в открытом стандарте RFC 2138 [4], основные особенности: клиентская часть RADIUS находится на Network Access Server'e и взаимодействует по сети с сервером RADIUS'a; все операции между клиентом RADIUS'a и сервером авторизуются посредством shared secret key который никогда не передается по сети, пароль пользователя, содержащийся в сообщениях RADIUS'a, шифруется; сообщения RADIUS содержат в себе информацию, закодированную в виде полей тип–длина–значение. Недостатки: аутентификатор запроса генерируется недостаточно случайно, т.е. возможна атака с предсказанием аутентификатора; простые запросы легко поддаются анализу с последующим перебором секретного ключа. Развитием протокола RADIUS стал протокол Diameter описанный в стандарте RFC 3588 [5], который исправлял недостатки своего предшественника.

Протокол EAP [6] предназначен для обеспечения расширенной аутентификации, когда IP протокол недоступен. Изначально предназначался для использования вместе с PPP (Point-to-Point Protocol) протоколом. Протокол EAP нашёл широкое применение в беспроводных сетях. Главной особенностью данного протокола является то, что механизм аутентификации определяется на более поздней фазе, уже после установления непосредственного соединения, что дает различный выбор между методами аутентификации. Но также это преимущество является и недостатком, т.к. развитие беспроводных сетей влекут за собой увеличение количества методов аутентификации, это приводит к тому что, протокол EAP не способен поддерживать современные методы аутентификации. Поэтому, был разработан протокол EAP-PSK, работающий поверх протокола EAP.

Заключение. Проанализировав протоколы сетевой аутентификации, можно прийти к единому выводу, что, не смотря на все преимущества каждого протокола отдельно взятого, каждый из них имеет свои недостатки. Поэтому лучше всего будет использовать протоколы не по отдельности, а в совокупности, что теоретически позволит перекрыть недостатки одного протокола преимуществом другого. Но у такого подхода есть недостаток, из-за того, что IoT маломощные вариант с комбинированием протоколов аутентификации может повлечь за собой сбои в работе устройств. Поэтому, основная задача сводится к поиску и реализации других подходов аутентификации устройств в сети, с применением различных протоколов аутентификации и механизмов идентификации устройств. В дальнейшем планируется более подробно изучить существующие методы и протоколы аутентификации, и их существующие реализации, провести исследование с обобщением полученных результатов.

ЛИТЕРАТУРА

1. Безопасность АСУ ТП: Итоги 2017 года // Positive Technologies. – 2018. [Электронный ресурс] – Режим доступа: <https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/ICS-Security-2017-rus.pdf> (дата обращения: 06.03.18).
2. Основные методы аутентификации [Электронный ресурс]. – Режим доступа: <http://сетиэвм.рф/attachments/article/62/Autentification-v1.pdf> (дата обращения: 07.03.18).
3. Протокол сетевой аутентификации Kerberos 5 [Электронный ресурс]. – Режим доступа: <https://www.ixbt.com/comm/kerberos5.shtml> (дата обращения: 09.03.18).
4. Willens S. et al. Remote authentication dial in user service (RADIUS). – 2000. – №. RFC 2138 [Электронный ресурс]. – Режим доступа: <https://tools.ietf.org/html/rfc2138> (дата обращения: 09.03.18).
5. Calhoun P. et al. Diameter base protocol. – 2003. – №. RFC 3588 [Электронный ресурс]. – Режим доступа: <http://www.faqs.org/rfcs/rfc3588.html> (дата обращения: 09.03.18).
6. Aboba B. et al. Extensible authentication protocol (EAP). – 2004. – № RFC 3748 [Электронный ресурс]. – Режим доступа: <http://www.protocols.ru/WP/wp-content/uploads/2014/03/rfc3748.pdf> (дата обращения: 10.03.18).

ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ ВЕБ-ПРИЛОЖЕНИЙ И МЕТОДЫ ЗАЩИТЫ ОТ НИХ

К.О. Семьехина, магистрант

*Научный руководитель Е.А. Шельмина, доцент каф. ЭМИС, к.ф.-м.н.
г. Томск, ТУСУР, каф. ЭМИС, semehinakseniya@mail.ru*

В современном мире деятельность любой организации так или иначе связана с веб-технологиями. Например, широкое распростране-

ние получили веб-порталы различных услуг (в том числе государственных), интернет-магазины, торговые площадки, различные бизнес-приложения, системы дистанционного банковского обслуживания. Невозможно представить себе современную организацию, будь то крупная корпорация или небольшая частная фирма, у которой не было бы своего официального сайта или странички на каком-либо публичном веб-ресурсе. Корпоративные приложения, для которых необходимо устанавливать клиентское ПО и регулярно его обновлять, уходят в прошлое. Веб-технологии позволяют значительно упростить бизнес-процессы [1].

Для того чтобы максимально использовать преимущества веб-технологий, необходимо обеспечить доступность ресурсов для целевой аудитории, например, из сети Интернет. Но доступ, следовательно, могут получить и злоумышленники. Это и недобросовестные конкуренты, и другие категории нарушителей, руководствующихся преступными намерениями, например, с целью хищения денежных средств, нарушения доступности ресурса или получения чувствительной информации. Компрометация приложений может привести как к репутационным потерям, так и к финансовым, в том числе в виде упущенной прибыли [1].

Разработка новых веб-приложений часто фокусируется на опыте заказчика и наиболее часто она сводится к обеспечению необходимой функциональности и качественного интерфейса для пользователей. Вопросами обеспечения безопасности в то же время часто пренебрегают или откладывают их решение на последнюю стадию – стадию тестирования приложения [1].

Цель представляемой работы заключается в проведении исследования существующих уязвимостей веб-приложений, способов их защиты и разработка собственного решения по организации защиты веб-приложения.

Уязвимости веб-приложений. В данной работе для проведения анализа уязвимостей веб-приложений были изучены статистические данные сообщества OWASP. Это сообщество ведет постоянно актуализируемый список OWASP Top 10, в котором перечислены наиболее опасные уязвимости в системе безопасности веб-приложений. Список OWASP Top 10 является лучшей практикой устранения уязвимостей веб-приложений. Список OWASP содержит перечень уязвимостей, отсортированных по степени их опасности [2]:

1. внедрение кода;
2. некорректная аутентификация и управление сессиями;
3. межсайтовый скриптинг;
4. небезопасные прямые ссылки на объекты;

5. небезопасная конфигурация;
6. утечка уязвимых данных;
7. отсутствие контроля доступа к функциональному уровню;
8. подделка межсайтовых запросов (CSRF);
9. использование компонентов с известными уязвимостями;
10. непроверенные перенаправления и переходы.

Методы защиты веб-приложений. Контрмеры по безопасности веб-приложений можно внедрять на двух этапах жизни приложения – разработки и эксплуатации. На этапе разработки – это различные инструменты тестирования безопасности: статический, динамический, интерактивный анализ. Если говорить о безопасности уже эксплуатируемого приложения, то здесь предлагается использовать налаженные средства защиты – системы предотвращения вторжений, межсетевые экраны следующего поколения (Next Generation Firewall, сокращенно NGFW), а также средства фильтрации трафика прикладного уровня, специально ориентированные на веб-приложения (Web Application Firewall, сокращенно – WAF). Применение Web Application Firewall традиционно считается наиболее эффективным подходом к защите веб-ресурсов. Одним из основополагающих факторов здесь служит узкоспециализированная разработка [3].

На сегодняшний день популярностью пользуются продукты компаний:

1. Imperva;
2. F5 Networks;
3. Barracuda Networks;
4. Citrix;
5. Positive Technologies;
6. Wallarm.

Однако несмотря на нацеленность производителей WAF на защищенность узкопрофильной области, каждый из них имеет свое видение и подход к защите частных инфраструктур. Тем самым грамотный подбор средства защиты является решающим моментом, ведь от того, насколько хорошо подходит средство для конкретной инфраструктуры, зависит его конечная эффективность [3].

По результатам сравнительного анализа можно сделать вывод, что рынок Web Application Firewall несмотря на свою многолетнюю историю все еще находится на этапе раннего развития. Поэтому планируется реализация собственного программного решения для защиты веб-приложений на языке программирования PHP.

Разрабатываемое приложение будет осуществлять мониторинг запросов к веб-приложению с целью предотвращения некорректных запросов, а также межсайтового скриптинга и межсайтовых запросов.

В данное приложение будет осуществляться проверка директории веб-приложения на наличие правил доступа к потенциально уязвимым данным, таким как файлы конфигурации приложения. Все это позволит эффективно защищать веб-приложение от наиболее распространенных уязвимостей из вышеупомянутого перечня угроз OWASP.

ЛИТЕРАТУРА

1. Web-Valneraby–2016-rus. [Электронный ресурс.] – Режим доступа: <https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Web-Vulnerability–2016-rus.pdf> (дата обращения: 24.12.2017).
2. IBM – в России и странах СНГ. Проверьте ваши приложения на уязвимости из списка OWASP Top 10 за 2013 г. [Электронный ресурс]. – Режим доступа: <https://www.ibm.com/developerworks/ru/library/se-owasp-top10/index.html> (дата обращения: 24.12.2017).
3. Обзор рынка защиты веб-приложений WAF в России и в мире. [Электронный ресурс.] – Режим доступа: https://www.anti-malware.ru/reviews/web_application_firewall_market_overview_russia (дата обращения: 24.12.2017).

СРАВНИТЕЛЬНОЕ ИССЛЕДОВАНИЕ МЕТОДОВ КЛАССИФИКАЦИИ В СТЕГОАНАЛИЗЕ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ПРИЗНАКОВ В ЧАСТОТНОЙ ОБЛАСТИ

О.О. Шумская, техник

*Научный руководитель О.О. Евсютин, доцент каф. БИС, к.т.н.
г. Томск, ТУСУР, каф. БИС, shumskaya.oo@gmail.com*

На сегодняшний день большая часть информации хранится в цифровом виде, в частности в цифровых изображениях: фотографии, картинки, отсканированные документы, графики и др. Ежедневно в сеть загружаются тысячи цифровых изображений, что приводит к возможности массового использования методов цифровой стеганографии, не всегда в законных целях. Стеганография – наука о способах передачи, хранения информации, обеспечивающих сокрытие наличия этой информации в некотором сигнале, предоставляет различные методы сокрытия данных в цифровых изображениях [1].

С целью обнаружения факта наличия секретных вложений в цифровых файлах применяются методы стегоанализа, представляющего собой науку о способах выявления фактов наличия скрытых сообщений в цифровых объектах.

Были рассмотрены известные работы по стегоанализу с использованием методов машинного обучения. Целью данной работы является проведение их сравнительного анализа.

Обзор работ по стегоанализу цифровых изображений с использованием методов машинного обучения. В общем случае стегоанализ цифровых объектов рассматривается как задача двухклассовой классификации, когда для каждого анализируемого объекта выбирается один из двух исходов: нет вложения или объект содержит скрытые данные.

Часто в работах применяют классификатор на основе линейного дискриминанта Фишера (ЛДФ), например, в [2]. Такой классификатор достаточно гибкий относительно количества рассматриваемых признаков, так как проецирует весь вектор признаков на прямую. Суть классификации заключается в поиске лучшего направления данной проекции, чтобы величину можно было однозначно отнести к определенному классу.

Авторы работ [3, 4] в качестве классификатора выбрали метод опорных векторов (support vector machine – SVM). Идея метода заключается в поиске такой прямой, которая наилучшим образом разделяет на классы точки из обучающей выборки, размещенные на плоскости. Далее все новые точки автоматически классифицируются следующим образом: точка выше прямой попадает в один класс, точка ниже прямой – в другой. Однако в пространствах высоких размерностей необходимо рассматривать гиперплоскости – пространства, размерность которых на единицу меньше, чем размерность исходного пространства.

В работе [5] авторы применяют для классификации нейронные сети. Общую схему функционирования сети можно описать следующим образом: набор признаков через входной слой проходит 2 слоя нейронов, на каждом из которых взвешивается согласно соответствующей слою матрице весов. Значения на выходе сравниваются с входным набором, выполняется проверка: «узнала» система образ или нет. Если «узнала», то изображение можно отнести к данному классу, если нет – сеть проверяет принадлежность изображения к другому классу, изменяя матрицы весов.

Авторы работ [6, 7] выбрали достаточно популярный в области стегоанализа наивный байесовский классификатор (НБК). Суть данного метода заключается в подсчете апостериорной вероятности на основе известных из обучения классификатора априорных вероятностей. При анализе конкретного изображения рассчитываются значения апостериорных вероятностей принадлежности данного изображения к каждому из двух рассматриваемых классов. Решение принимается на основании сравнения двух рассчитанных вероятностей.

В некоторых работах можно встретить метод стегоанализа с классификатором на основе автоматического многослойного персеп-

трона (AutoMLP) [8, 9]. AutoMLP – простой алгоритм, повышающий темп обучения и регулирующий размер нейронных сетей во время обучения; включает идеи генетических алгоритмов и стохастической оптимизации. Суть заключается в поддержании малого числа сетей, которые обучаются параллельно с различными уровнями и различными числами скрытых модулей. После малого постоянного числа временных шагов определяется коэффициент ошибок, и худшие экземпляры заменяются копиями лучших сетей, измененных подобно мутации в генетическом алгоритме. У метода есть настраиваемые параметры: количество шагов (S), поколений (G) и ансамблей нейронных сетей, обучающихся параллельно (E).

Эксперименты. В качестве исследуемых изображений подготовлены 863 полутоновых сжатых JPEG-изображения размером 256×256 : стандартные изображения (Lena, Splash, Peppers, Boat и т.п.) и экземпляры из баз изображений UCID (Uncompressed Colour Image Database) [10] и USC-SIPI ID (University of Southern California Signal and Image Processing Institute Image Database) [11]. Выборка содержит 411 изображений без вложения (чистые, пустые) и 452 с вложением по одному из методов (Jsteg, PM1, F5).

В качестве признакового набора были выбраны характеристики в частотной области: 3 признака на основе соотношений энергий, собранных в отдельных частотных ДКП-коэффициентах (1) [6] и 3 двойные гистограммы АС-коэффициентов со значениями $\{-1, 0, 1\}$ [12, 13].

$$F(1) = \frac{E(f_0)}{E(f_{|\eta|=1})}, \quad F(2) = \frac{\sum_{|\eta|>1} E(f_{\eta})}{E f_{|\eta|=1}}, \quad F(3) = \frac{En_{|\eta|>1}}{En f_{|\eta|\leq 1}}, \quad (1)$$

где $E(f_0)$ – среднее значение частоты встречаемости АС-коэффициентов, равных 0, по всем блокам изображения; $E(f_{|\eta|=1})$ – среднее значение частоты встречаемости тех АС-коэффициентов изображения, абсолютная величина которых равна 1, по всем блокам изображения; $En_{|\eta|>1}$ – энергия тех АС-коэффициентов изображения, абсолютная величина которых больше 1.

Точность методов (табл.) показывает, что наиболее подходящие методы – это ЛДФ, AutoMLP ($S=20$, $G=20$, $E=4$) и нейронные сети (разница $< 0,35\%$). По точности обнаружения изображений без вложения AutoMLP имеет преимущество перед нейронными сетями на 6,67% и перед ЛДФ на 4,16%. По точности обнаружения изображений с вложением нейронные сети имеют преимущество перед AutoMLP на 6,36% и перед ЛДФ на 1,88%.

Результаты классификации

Классификатор	Доля верно классифицированных изображений, %		Точность, %
	с вложением	без вложения	
AutoMLP ($S=20, G=20, E=4$)	75,27	63,89	69,58
AutoMLP ($S=15, G=15, E=4$)	95,57	31,25	64,90
НБК	71,51	60,44	65,98
Нейронные сети	81,63	57,22	69,42
ЛДФ	79,75	59,73	69,74
SVM	77,24	55,57	66,41

Среди рассмотренных вариантов можно было бы выбрать средний по точности вариант – ЛДФ, однако с поправкой на стремление стегоанализа увеличить вероятность обнаружения изображений с вложением, наиболее подходящий метод – нейронные сети.

Отдельные эксперименты показали, что AutoMLP обеспечивает очень высокую точность обнаружения изображений с вложением (более 95%) при $S = 15, G = 15, E = 4$. В спорных ситуациях или при наличии сомнения в решении можно воспользоваться дополнительной проверкой с помощью метода AutoMLP.

ЛИТЕРАТУРА

1. Конахович Г.Ф. Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. – 288 с.
2. Jia-Fa M. A steganalysis method in the DCT domain / M. Jia-Fa, N. Xin-Xin, X. Gang, Sh. Wei-Guo, Zh. Na-Na // Multimedia Tools and Applications. – 2016. – №75. – P.5999–6019.
3. Xia Zh. Steganalysis of LSB matching using differences between nonadjacent pixels / Zh.Xia, X. Wang, X. Sun, Q. Liu, N. Xiong. // Multimedia Tools and Applications. – 2016. – P. 1947–1962.
4. Fusheng Y. Novel Image Splicing Forensic Algorithm Based on Generalized DCT Coefficient-Pair Histogram / Y. Fusheng, T. Gao // Proceedings of 10th Chinese Conference (IGTA 2015). – China, Beijing. – 2015. – P. 63–71.
5. Zong H. Blind image steganalysis based on wavelet coefficient correlation / H. Zong, F. Liu, X. Luo // Digital Investigation. – 2012. – Vol. 9. – P. 58–68.
6. Berg G. Searching For Hidden Messages: Automatic Detection of Steganography / G. Berg, I. Davidson, M.-Y. Duan, G. Paul // Proceedings of the 15th Innovative Applications of Artificial Intelligence (IAAI) Conference, August 12–14. – 2003. – Acapulco, Mexico. – P. 51–56.
7. Maitra S. New Results on Generalization of Roos-type Biases and Related Keystream of RC / S.Maitra, G. Paul, S.Sarkar, M. Lehmann, W. Meier // Proceedings of the 6th International Conference on Cryptology in Africa (AFRICACRYPT), June 22–24. – 2013. – Cairo, Egypt. – Vol. 7918. – P. 222–239.
8. Sabeti V. Steganalysis and payload estimation of embedding in pixel differences using neural networks / V. Sabeti, Sh. Samavi, M. Mahdavi, Sh. Shirani // Pattern Recogn. – 2010. – №43 (1). – P. 405–415.

9. Lubenko I. Steganalysis with mismatched covers: Do simple classifiers help? / I. Lubenko, A.D. Ker // Proceedings of the on Multimedia and Security, MM&Sec'12, September 6–7. – 2012. – New York, NY, USA. – P. 11–18.
10. Image Databases [Electronic recourse] // ImageProcessingPlace.com. – Electronic data. – URL: http://www.imageprocessingplace.com/root_files_V3/image_databases.htm
11. SIPI Image Database [Electronic recourse] // USC University of Southern California. – Electronic data. – Los Angeles, CA, 2017. – URL: <http://sipi.usc.edu/database>.
12. Fridrich J. Feature-Based Steganalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes / J. Fridrich // Proceedings of the Sixth International Workshop on Information Hiding, Lecture Notes in Computer Science. – 2014. – Vol. 3200. – P. 67–81.
13. Chen M.-C. Alpha-trimmed Image Estimation for JPEG Steganography Detection / M.-C. Chen // Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics. – San Antonio, Texas, USA. – 2009. – P. 4581–4585.

НАПОЛНЕНИЕ И ПРЕДОБРАБОТКА БАЗЫ ДАННЫХ КЛАВИАТУРНОГО ПОЧЕРКА

Д.С. Световец, студент; Е.Ю. Костюченко, доцент

г. Томск, ТУСУР, каф. КИБЭВС, lehpflehpf@gmail.com,

*Проект ГПО КИБЭВС-1005 «Система распознавания образов
на основе нейронных сетей»*

Клавиатурный почерк – уникальная характеристика, присущая каждому человеку. Чтобы составить персональный профиль, современным системам необходимо проанализировать динамику набора текста, оценить скорость набора текста, размеры интервалов между нажатиями и время удержания клавиш [1].

Основные задачи данного этапа. В качестве основной задачи данного этапа выступает наполнение базы данных клавиатурного почерка, анализ полученной базы данных и её модификация с целью устранения длительных перерывов в процессе набора и значений от длительное время непрерывно удерживаемых клавиш.

Реализация. Заполнение базы клавиатурного почерка проходило с помощью специальной программы. Она считывала какая клавиша была нажата, время нажатия этой клавиши и время, когда данная клавиша была отпущена.

На рис. 1 представлен фрагмент базы клавиатурного почерка. В первом столбце отображается id пользователя, во втором id сессии, в третьем id клавиши, в четвёртом нажата ли клавиша в этот момент

или отпущена (1 и 2 соответственно), а в пятом – момент времени, когда это произошло.

	1	2	3	4	5	6
1587076	15	3	191	2	6364384341...	
1587077	15	3	32	1	6364384341...	
1587078	15	3	32	2	6364384341...	
1587079	15	3	189	1	6364384341...	
1587080	15	3	189	2	6364384341...	
1587081	15	3	32	1	6364384341...	

Рис. 1. Пример значений параметров

Текущее наполнение базы – 13 пользователей с более 180000 сигналами от клавиш от каждого пользователя (сигнал – время нажатия-отпускания) до проведения нижеописанной предобработки.

На основе полученных данных для каждой клавиши были рассчитаны времена удержания, которые вычислялось как интервал времени с момента, как была нажата клавиша, до момента, как клавиша была отпущена. Затем были вычислены интервалы времени с нажатия одной клавиши до момента нажатия другой клавиш отдельно для каждого пользователя.

Полученные данные необходимо было преобразовать для дальнейшей работы с ними. Было принято решение значения для каждого пользователя вывести в отдельные таблицы, в них хранится информация о времени с момента нажатия одной клавиши, до момента нажатия следующей.

На рис. 2 в первом столбце отображается идентификатор первой нажатой клавиши, во втором столбце – идентификатор следующей нажатой клавиши, в третьем столбце отображается время с момента нажатия первой клавиши до времени нажатия второй, а в четвёртом столбце отображается номер сессии. По полученным данным была построена гистограмма (рис. 3).

f_tab{2, 15}				
	1	2	3	4
1	160	68	297	1
2	68	32	120	1
3	32	160	272	1
4	160	68	143	1

Рис. 2. Фрагмент полученной таблицы для пользователя № 15

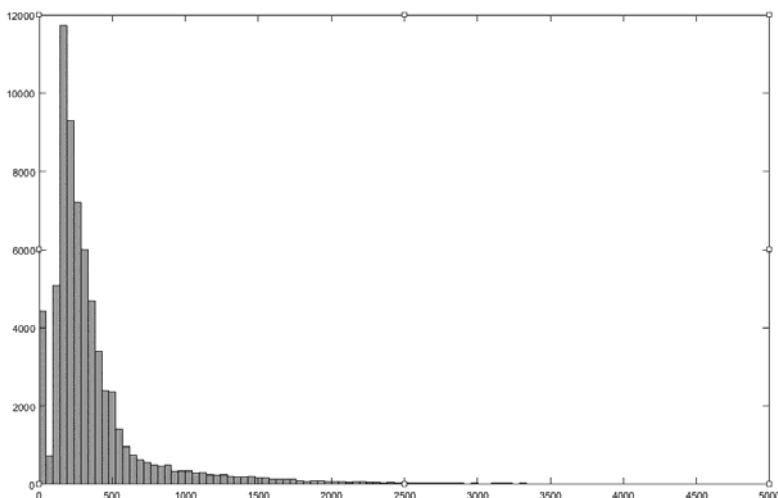


Рис. 3. Гистограмма времен между нажатиями клавиш

На гистограмме (см. рис. 3) по оси x рассматривается время с нажатия одной клавиши до нажатия до другой в миллисекундах, а на оси y количество этих времён, входящих в интервал. На полученной гистограмме видно, аномально большое значения для времени меньше 100, оно связано с тем, что если клавишу зажать, то программа считает это как множественное нажатие одной и той же клавиши. Также видно, что наблюдаются значения для больших времён, они обусловлены наличием пауз в наборе текста, а не статистическими характеристиками данных значений.

Было принято решение, для значений времени меньше 100 произвести обработку. То есть если время с момента нажатия одной клавиши и нажатия следующей за ней меньше 100, а клавиши одинаковые, то в базу записывается общее время удержания клавиши до того момента пока не будет нажата другая клавиша. Также при времени больше 5000 с момента нажатия одной клавиши и нажатия следующей за ней искусственно прерываем сессию и начинаем новую, аргументировав это перерывом в процессе набора текста. В результате была построена гистограмма времен для предобработанного текста (рис. 4).

На полученных данных была произведена проверка их принадлежности к какому-либо распределению из следующего списка: гамбеловское; экспоненциальное; гамма; логнормальное; нормальное; рэлеевское; равномерное; вейбулловское. Ни одна проверка не оказа-

лась положительной, однако по виду распределения появилась возможность говорить о его одномодальности.

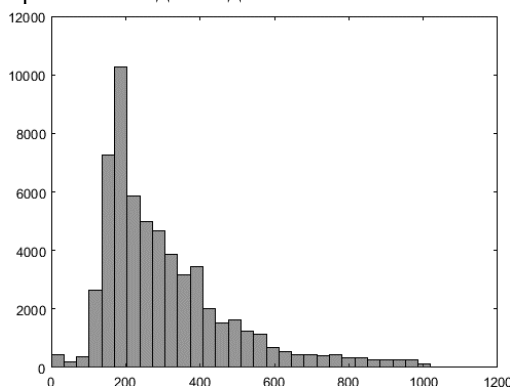


Рис. 4. Гистограмма после преобразований

Заключение. По итогу проделанной работы была наполнена и модифицирована база данных клавиатурного почерка с учетом выявленных аномальных значений и объяснения причин их возникновения. На следующем этапе будет рассматриваться возможность обучения нейронной сети по данной базе данных клавиатурного почерка, с целью определения пользователя.

Проект выполнен в рамках базовой части государственного задания министерства образования и науки Российской Федерации на 2017–2019 гг. Номер 8.9628.2017/8.9

ЛИТЕРАТУРА

1. Распознавание клавиатурного почерка [Электронный ресурс]. – Режим доступа: <https://stakhanovets.ru/blog/raspoznavanie-klaviaturnogo-pocherka-ugroza-anonimnosti-v-seti/> (дата обращения: 18.02.2018).

ПОДСЕКЦИЯ 4.2

РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ И СРЕДСТВА ИХ ЗАЩИТЫ

*Председатель секции – Голиков А.М., доцент каф. РТС, к.т.н.;
зам. председателя – Бернгардт А.С., доцент каф. РТС, к.т.н.*

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ СИСТЕМЫ АНТИКРИЗИСНОГО УПРАВЛЕНИЯ МЧС РОССИИ

*Н.Е. Аносинская, магистрант; О.С. Каймонов, аспирант
г. Томск, ТУСУР, N каф. ТУ, ataliaAnosinskaya@mail.ru*

В современном мире, важнейшим элементом созданной и действующей в стране единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (ЧС) является система антикризисного управления в ЧС, представляющая собой оперативную составляющую российской единой системы предупреждения и ликвидации чрезвычайных ситуаций (РСЧС). Основу системы антикризисного управления в чрезвычайных ситуациях составляют органы повседневного управления, постоянно действующие органы управления функциональных и территориальных подсистем РСЧС, оперативные штабы и оперативные группы, формируемые на время ликвидации ЧС [1].

Цель работы – предложить варианты по улучшению функциональных возможностей сетевого оборудования.

Антикризисное управление – это система управления, которая имеет комплексный, системный характер и направлена на предотвращение или устранение неблагоприятных явлений посредством использования всего потенциала современных технологий, разработки и реализации специальных программ, совершенствования систем взаимодействия и функционирования объектов и субъектов. Она позволяет повысить оперативность реагирования, а также эффективность применения сил и средств и уменьшений ущерба [2].

В 2009 г. сформирована структура системы антикризисного управления, организационно – техническую основу которой составляют: национальный центр управления в кризисных ситуациях (НЦУКС), центры управления в кризисных ситуациях (ЦУКС) территориальных органов МЧС России, органы повседневного управления

федеральных органов исполнительной власти, единая дежурно-диспетчерская служба (ЕДДС) муниципальных образований и единая дежурно-диспетчерская служба (ДДС) организаций.

Основными задачами НЦУКС МЧС России являются: завершение вертикали антикризисного управления в рамках РСЧС, включающие территориальные и функциональные подсистемы на уровне муниципальных образований и гарнизонов пожарной охраны; нормативное правовое обустройство деятельности ЦУКС главных управлений МЧС России по субъектам Российской Федерации, как головных органов повседневного управления в составе подсистем РСЧС; совершенствование системы космического мониторинга; реализация паспортов территорий как единого информационного ресурса для федеральных органов исполнительной власти Российской Федерации; внедрение системы многофакторного моделирования возможных ЧС с учетом рисков, присущих территориям; оперативное управление действиями подразделений при выполнении мероприятий по экстренному предупреждению и ликвидации ЧС; координация деятельности органов повседневного управления РСЧС при угрозе возникновения ЧС; сбор, обработка и предоставление органами управления РСЧС оперативной информации о ЧС, организация мониторинга и прогнозирования ЧС, а также учет сил и средств, ресурсов, задействованных для ликвидации ЧС [1]. На рисунке 1 показана система антикризисного управления.



Рис. 1. Система антикризисного управления

Для выполнения вышеперечисленных задач, создана мультисервисная транспортная сеть, включающая в себя несколько компонентов, исполняющих различные по функционалу задачи. На рис. 2 показана информационная составляющая системы антикризисного управления.

ИНФОРМАЦИОННАЯ СОСТАВЛЯЮЩАЯ СИСТЕМЫ АНТИКРИЗИСНОГО УПРАВЛЕНИЯ

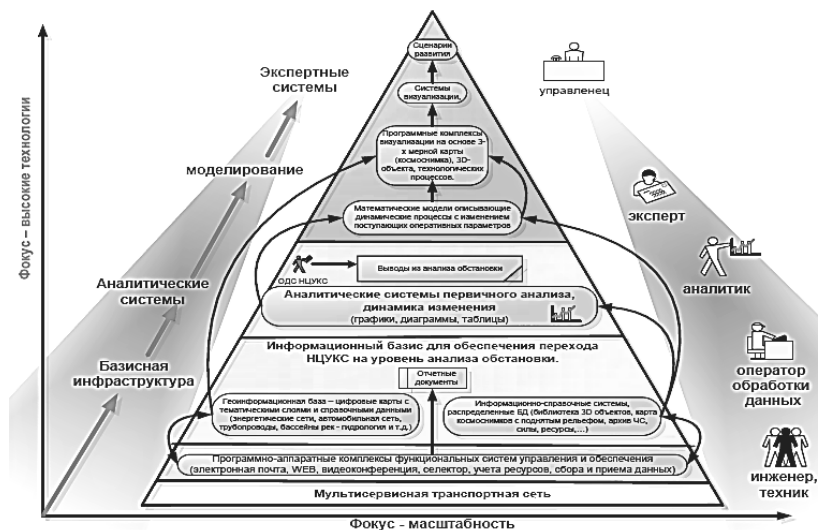


Рис. 2. Структура мультисервисной транспортной сети

Мультисервисная сеть МЧС России (МС) – это сеть связи, построенная в соответствии с концепцией NGN и обеспечивающая предоставление неограниченного набора услуг.

Мультипротокольная сеть – транспортная сеть связи, входящая в состав МС, обеспечивающая перенос разных видов информации с использованием различных протоколов передачи.

Мультисервисная сеть представляет собой универсальную многоцелевую среду, предназначенную для передачи речи, изображения и данных с использованием технологии коммутации пакетов (IP). МС отличается степенью надежности, характерной для телефонных сетей и обеспечивает низкую стоимость передачи в расчете на единицу объема информации.

Основная задача МС заключается в обеспечении работы разнообразных информационных и телекоммуникационных систем и приложений в единой транспортной среде, когда для передачи обычного трафика (данных) и трафика другой информации, используется единая инфраструктура [3].

Построение МС осуществляется на базе самых различных технологий, как на платформе IP (IP VPN), так и на базе выделенных каналов связи. На магистральном уровне наиболее популярны сегодня технологии IP/MPLS, Packet over SONET/SDH, POS, ATM, xGE, DWDM, CWDM, RPR.

Мультисервисная сеть МЧС России – это единая цифровая сеть, способная передавать голос, видеоизображения и данные.

Непрерывное улучшение основных технологий выражает стремление к созданию единой общей технологической базы, для построения сетей связи и способной удовлетворить требованиям и региональных сетей связи, и локальных вычислительных сетей.

В связи с нестабильной ситуацией в мире, тот факт, что МС построена на различных программных продуктах, не гарантирует стабильную работу и качество передачи, не говоря о сложности реализации данной сети и дорогой стоимости компонентов. Эти факторы затрудняют работу и создание таких сетей.

Таким образом, совершенствование МС будет заключаться в том, чтобы привести всю систему к единой платформе, построенную на отечественных компонентах и программных продуктах.

Данное решение позволит расширить функциональные возможности сетевого оборудования, уменьшит стоимость владения и поддержание сложных мультимедиа.

ЛИТЕРАТУРА

1. Мероприятия по смягчению последствий чрезвычайных ситуаций [Электронный ресурс]. Режим доступа: <http://en.mchs.ru/upload/site1/activities/results/6.1.GosDoklad2011.pdf> (дата обращения: 07.03.2018).

2. Система антикризисного управления МЧС России [Электронный ресурс]. Режим доступа: https://revolution.allbest.ru/management/00618376_0.html (дата обращения: 09.03.2018).

3. Понятие мультисервисных сетей связи. [Электронный ресурс]. Режим доступа: <https://lektsii.org/6-41911.html> (дата обращения: 12.03.2018).

РАСПОЗНАВАНИЕ ЛИЦ ЛЮДЕЙ ПО СИГНАЛАМ С КАМЕРЫ ВИДЕОНАБЛЮДЕНИЯ

Р.В. Блесков, студент

*Научный руководитель А.М. Голиков, доцент каф. РТС, к.т.н., с.н.с.
г. Томск, ТУСУР, каф. РТС, rts2_golikov@mail.ru*

Обнаружение лиц представляет собой систему, включающую набор функций, позволяющих решать задачи обнаружения лиц, определения их положения на цифровом изображении, а также межкадрово-

го прослеживания наблюдаемых лиц в реальном масштабе времени. Процедура обнаружения лица выделяет человеческое лицо на черно-белых или цветных изображениях во фронтальной или околофронтальной проекции и возвращает координаты объемлющих прямоугольников для всех обнаруженных лиц. Процедура слежения за лицами позволяет накапливать и сохранять в системе информацию о лице человека (последовательность изображений лица с различными ракурсами и выражениями) до тех пор, пока лицо не выйдет из зоны наблюдения или не отвернется от камеры.

Система распознавания лица представляет собой программно-алгоритмический комплекс, решающий задачи верификации и идентификации пользователя на основе сравнительного анализа предъявляемого лица. Процедура верификации предусматривает сравнение предъявляемого лица с выбранным лицом, хранящимся в текущей базе данных. Процедура идентификации предусматривает проверку принадлежности предъявляемого лица ко всей базе данных лиц или заранее оговоренной ее части. Система включает в себя набор алгоритмов автоматической верификации и идентификации лиц, обеспечивающих биометрическое распознавание пользователя с вероятностью до 95%. Наличие интерфейса настраиваемых параметров работы алгоритмов, спектр методов распознавания лиц, эффективные алгоритмы предобработки, возможность оптимизации решения под аппаратные требования заказчика и многое другое позволяют использовать данное решение как удобное и гибкое средство по созданию клиент-ориентированных биометрических систем [1–2].

Тестовая программа распознавания лиц обрабатывает 2D-изображения. На рис. 1 представлен интерфейс программы с загруженной в неё фотографией.

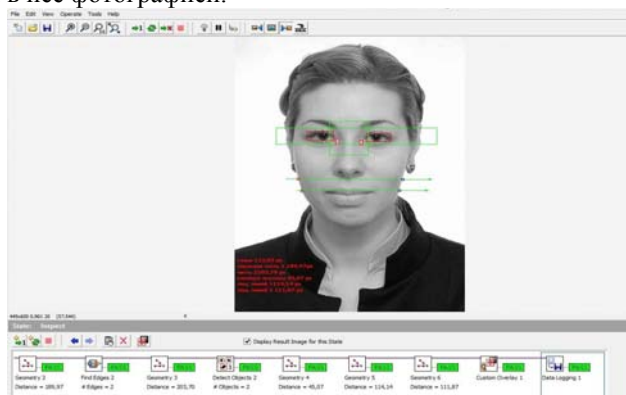


Рис. 1. Программа распознавания лиц

Программа разработана в одном из пакетов LabView, это NI Vision Builder. Данный пакет позволяет составлять различные схемы, которые могут производить фото и видеообработку, различной сложности.

Системы распознавания лиц делятся две категории – двухмерные (в их основе лежат плоские, или двухмерные, изображения, 2D) и трехмерные (распознавание производится по реконструированным трехмерным образам, 3D). Однако, системы 2D-распознавания очень чувствительны к условиям освещенности. При неравномерном освещении лица достоверность 2D-распознавания заметно снижается. В то время как для систем 3D-распознавания изменения в освещенности влияют лишь на текстуру лица, а реконструированная поверхность лица остается неизменной. И в тех и в других системах для распознавания лиц применяются устойчивые антропометрические точки, расположение которых характеризует индивидуальные особенности лица. На 3D-моделях антропометрические точки определяются с большей точностью, чем на 2D-изображениях. Также, точки на 3D-моделях имеют три координаты и, поэтому, предоставляют больше информации, чем те такие же точки на 2D-изображении.



Рис. 2. Пример реконструирования лица в 3D формате

Разработанная система обладает следующими характеристиками:

1. Система производит распознавание лиц в режиме реального времени, и для этого человеку не нужно останавливаться перед ней. Построение модели происходит за 0,05 или 0,1 с.
2. Система производит сравнение 3D-модели с изображениями или эталонными моделями, проверяет их на совпадение, далее уве-

домляет об этом оператора или систему охраны в автоматическом режиме.

3. Система обладает устойчивостью к поворотам головы и различным мешающим видеонаблюдению и распознаванию факторам (тьма, различная освещенность, поворот головы и т.д.) [2].

ЛИТЕРАТУРА

1. Бенкренов В.А., Шмяков А.М. Цифровая обработка многомерных сигналов. – Ярославль: Изд-во ЯГУ им. П.Г. Демидова.

2. Брилюк Д.В, Старовойтов В.В. Распознавание человека по изображению лица нейросетевыми методами. – Минск: Изд-во Наука, 2002. – 52 с.

РАЗРАБОТКА ЛАБОРАТОРНО-ПРОГРАММНОГО КОМПЛЕКСА И УЧЕБНО-МЕТОДИЧЕСКОГО ПОСОБИЯ ДЛЯ ИЗУЧЕНИЯ ПРИНЦИПОВ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

С.Р. Еремеев, студент

Научный руководитель А.С.Бернгардт, доцент каф. РТС, к.т.н.

г. Томск, ТУСУР, каф. РТС, sergey_415@mail.ru

Проект ГПО РТС–1506 «Программный комплекс

для изучения перспективных методов кодирования и модуляции»

Основной задачей при выполнении данной работы является разработка алгоритмов и программ для последующего создания на их базе совокупности дидактических (демонстрационных) модулей для использования при проведении занятий по дисциплинам инфокоммуникационного профиля на кафедре РТС ТУСУР. Важнейшим требованием является возможность наглядного представления алгоритмов обработки сигналов. Это намного облегчает и ускоряет процесс изучения и освоения нового материала.

Существующее в настоящее время широко распространенное программное обеспечение (ПО), например, Matlab, предоставляет возможность эмуляции систем помехоустойчивого кодирования, позволяя рассматривать их только как некоторое подобие черного ящика, имеющего что-то на входе и выходе. Процессы, протекающие внутри него, скрыты от пользователя. Это затрудняет понимание тех алгоритмов и методов, которые являются ядром происходящих в нём преобразований. Это плохо, так как в ходе обучения главным является именно понимание алгоритмов преобразования сигналов и возможностей их аппаратурной и программной реализации.

На первом этапе решения поставленной задачи разработан программный комплекс, дающий наглядное представление о работе кодеров и декодеров систематического циклического кода Хэмминга с длиной кодового слова $n = 7$, количеством информационных символов $k = 4$, и, соответственно, числом проверочных символов $r = 3$.

Реализован алгоритм формирования систематического циклического кода [1]

$$s(x) = x^r a(x) + [x^r a(x)] \bmod g(x), \quad (1)$$

где $s(x)$ – полином кодового слова на выходе кодера; $a(x)$ – полином информационной последовательности на входе кодера; $g(x)$ – производящий полином.

Производящий полином в описываемой реализации программы имеет вид

$$g(x) = x^3 + x + 1.$$

Аппаратно операция $[x^r a(x)] \bmod g(x)$ реализуется на базе рекурсивного линейного цифрового фильтра.

Декодер циклического кода реализует алгоритм деления полинома комбинации на входе на производящий полином. Остаток от деления, являющийся признаком наличия ошибки, называют синдромом. Алгоритм декодирования имеет вид

$$\text{res}(x) = v(x) \bmod g(x), \quad (2)$$

где $v(x) = s(x) + e(x)$, $e(x)$ – полином вектора ошибок.

Один цикл кодирования можно описать следующим образом. В течение первых четырех тактов ключ находится в положении, соединяющим вход кодера с цепью обратной связи (ОС). На вход кодера и, вместе с тем на выход, поступают информационные символы. В это же время в регистре сдвига начинается процесс вычисления остатка от деления полинома $x^r a(x)$ на полином $g(x)$. После того, как четыре информационных символа были поданы, вход «отключается». Ключ переходит в положение, соединяющее выход регистра сдвига с выходом кодера. Для завершения процесса кодирования и вывода (подачи на выход) из регистра сдвига результата деления, необходимо продолжать в течение трех тактов подавать на схему тактовые импульсы. На седьмом такте кодовая комбинация уже сформирована.

Особенность данного программного модуля состоит в том, что весь процесс кодирования можно проследить по тактам. Можно непосредственно увидеть, как при этом меняются состояния ячеек регистра сдвига (триггеров), что передается по цепи ОС, что имеем на входе, и что впоследствии имеем на выходе.

Декодирование в программном модуле осуществляется в следующем порядке. На вход поступает декодируемая комбинация. В течение семи тактов в декодере происходит вычисление остатка (син-

дрома). Синдром определяется содержимым ячеек регистра сдвига на седьмом такте. Если на седьмом такте во всех ячейках регистра сдвига окажутся нули, значит, скорее всего, в комбинации на входе декодера ошибок нет. Можно вводить следующую декодируемую кодовую комбинацию. Если хотя бы в одной ячейке регистра сдвига будет «1», ошибки есть наверняка. Тогда осуществляется процесс поиска номера ошибочного символа. Номер такта, на котором в регистре сдвига появляется комбинация «100», определяет положение ошибочного символа, подлежащему исправлению. На этом процесс декодирования считается завершенным.

Помимо двух описанных оконных приложений, было разработано ещё одно, имеющее консольный интерфейс, и позволяющее исследовать статистические свойства рассматриваемого кода. В соответствии с битовой вероятности ошибки (BER) на входе декодера (выходе демодулятора) генерируется вектор независимых ошибок – поток нулей и единиц. Этот поток разбивается на блоки по семь символов и декодируется. Анализируя полученные результаты декодирования, можно составить отчетливое представление о том, ошибки какой кратности q декодер гарантированно обнаружит ($q = 1, q = 2, q = 5, q = 6$), какие может пропустить ($q = 3, q = 4$), а какие не заметить вовсе ($q = 7$).

Логическим завершением данной работы стала разработка учебно-методического пособия, вобравшего в себя краткие теоретические сведения по теме кодирования циклическими кодами, примеры применения рассматриваемых алгоритмов для практического решения расчетных задач, описание лабораторно-программного комплекса, расчетное задание, задание на лабораторную работу и контрольные вопросы.

Таким образом, в ходе проделанной работы был разработан лабораторно-программный комплекс, включающий в себя три демонстрационных модуля, и составлено учебно-методическое пособие, которые используются в учебном процессе.

Модули позволяют наблюдать процессы кодирования и декодирования с контролем состояния кодера и декодера, то есть содержимого всех триггерных ячеек. На примере декодера можно так же изучать работу генератора псевдо случайной последовательности (М-последовательности). Разработанное учебно-методическое пособие в сопряжении с лабораторно-программным комплексом позволяют максимально упростить знакомство с принципами помехоустойчивого кодирования на примере систематического циклического кода.

На сегодняшний день работа в данном направлении продолжается. В перспективе стоит разработка новых программных модулей, позволяющих исследовать коды большей длины, как систематических, так и несистематических.

ЛИТЕРАТУРА

1. Акулиничев Ю.П., Бернгардт А.С. Теория и техника передачи информации: учеб. пособие. – Томск: Эль Контент, 2012. – 210 с.

ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ИЗУЧЕНИЯ ПЕРСПЕКТИВНЫХ МЕТОДОВ КОДИРОВАНИЯ

А.О. Эрлих, А.В. Тетерлева, студенты

Научный руководитель А.С. Бернгардт, доцент каф. РТС, к.т.н.

г. Томск, ТУСУР, каф. РТС, asbern48@mail.ru

Проект ГПО РТС-1506 «Программный комплекс для изучения перспективных методов кодирования. Турбокодер»

Турбокод – это параллельный каскадный блочный систематический помехоустойчивый код, способный исправлять ошибки, возникающие при передаче цифровой информации по каналу связи с шумами.

Турбокод состоит из каскада параллельно соединённых систематических кодов. Эти составляющие называются компонентными кодами. В качестве компонентного кода использовался сверточный код.

Одним из вариантов построения турбо-кода является использование под кодера, на основе которого и будет построен сам турбо-код. Таким под кодом может быть сверточный кодер. Турбо-код будет построен на параллельном каскадировании двух сверточных кодов.

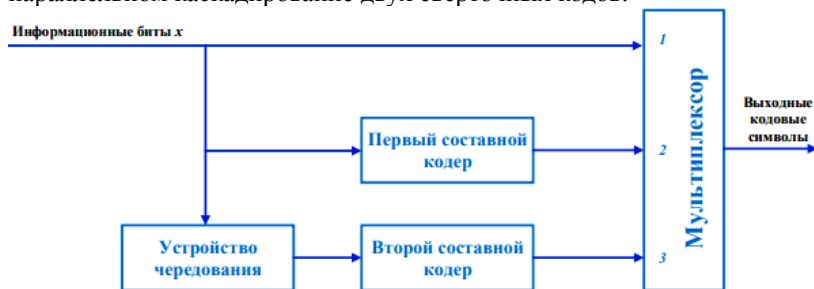


Рис. 1. Схема турбо-кодера

Информационный блок из N информационных бит (x) одновременно поступает на первый вход мультиплексора, на вход первого составного кодера и через устройство перемежителя на вход второго составного кодера.

С помощью перемежителя входной блок подвергается перестановке информационных символов, что позволяет минимизировать риск возникновения пакетов ошибок и формирует максимально независимые кодовые слова.

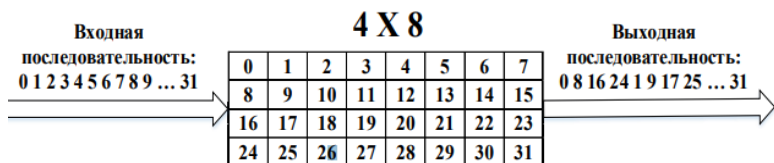


Рис. 2. Принцип работы устройства чередования

Переमेжение выполняется с помощью последовательного заполнения строк матрицы 4×8 кодированными символами и вывода блоков на второй составной кодер по столбцам.

Сформированные проверочные символы с первого (y1) и второго (y2) кодера поступают соответственно на второй и третий входы мультиплексора, который формирует поток кодовых символов в систематическом виде (xy1y2 xy1y2...).

Кодирование турбо-кода основано на работе двух параллельных рекурсивных систематических сверточных кодеров скорости $R = 1/2$ (это означает, что на информационный бит на входе RSC кодер откликается двумя битами на выходе). Структура сверточного кодера задается порождающими полиномами [1. 510]

$$\begin{aligned} g_1(x) &= 1 + x^2 + x, \\ g_2(x) &= 1 + x^2. \end{aligned} \quad (1)$$

Программный модуль разработан в программе Microsoft Visual C++, среда разработки приложений на языке C++, разработанная корпорацией Microsoft.

Пользователь вводит сообщение, далее программа переводит полученное сообщение в цифровой вид с использованием международной таблицы Unicode, после переводит сообщение в двоичный код.

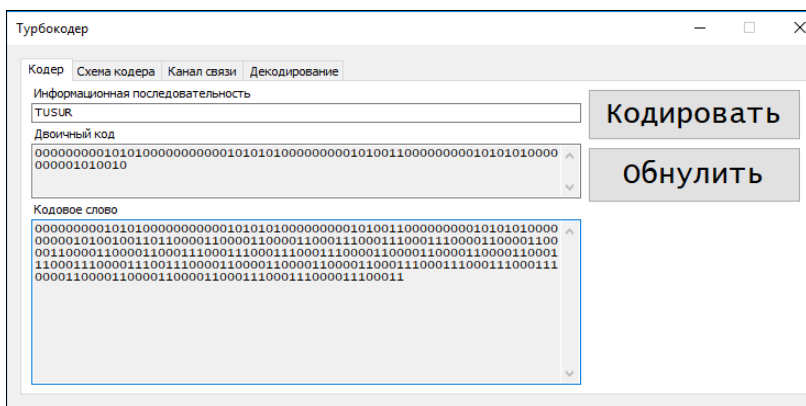


Рис. 3. Программный модуль

Схема реализованного трубокда изображена на рис. 4. Кодер состоит из двух параллельно соединенных сверточных кодеров, переключателя (INT) и мультиплексора (MUX).

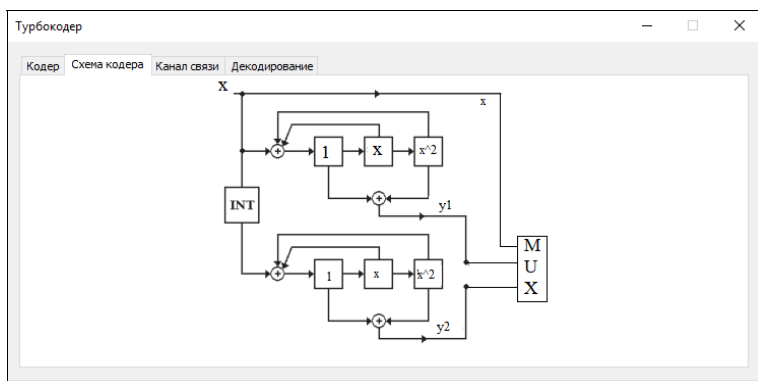


Рис. 4. Программный модуль

С помощью окна «BER %» можно указать процент возникновения ошибки символа, во время передачи символа в канале связи. Два других окна подсчитывают полное количество символов, передаваемых по каналу связи и количество ошибочных символов. Пример реализации такой возможности представлен на рис. 5.

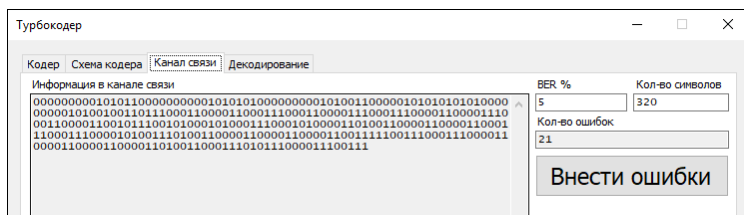


Рис. 5. Программный модуль

ЛИТЕРАТУРА

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М.: Вильямс. – 2007. – 1104 с.
2. Акулиничев Ю.П., Бернгардт А.С. Теория и техника передачи информации: учеб. пособие. – Томск: Эль Контент, 2012. – 210 с.
3. Зигангиров К.Ш., Кабатянский Г.А. Современная теория кодирования: учеб. пособие.
4. Никитин Г.И. Сверточные коды: учеб. пособие. – СПб., 2001.

ДИДАКТИЧЕСКИЙ МОДУЛЬ «КОДЕК РИДА–СОЛОМОНА (7,3)»

О.Ю. Григорьев, студент

*Научный руководитель А.С. Бернгардт, доцент каф. РТС, к.т.н.,
г. Томск, ТУСУР, каф. РТФ, gou_123-2@mail.ru, asbern48@mail.ru
ГПО РТС-1506 «Программный комплекс для изучения перспективных
методов кодирования и модуляции»*

Для защиты информации от помех широко применяются помехоустойчивые (корректирующие) коды Рида–Соломона, они позволяют исправлять пакеты ошибок кратности t .

В теории кодов Рида–Соломона важное место занимает понятие конечного поля, на котором они основаны, или поле Галуа – поле, состоящее из конечного числа элементов. Число элементов в поле называется его порядком. Конечное поле обозначается $GF(p^m)$, где p – простое число, а m – любое натуральное число. Например, для поля Галуа размерности 8, т.е. $GF(8)$, все математические операции будут происходить с числами $0, a^0, a^1, a^2, a^3, a^4, a^5, a^6$. В векторном виде 000, 010, 001, 110, 011, 111, 101, 100. Все операции в конечном поле выполняются по модулю. Таким образом, результат любой операции также является элементом данного поля. Для работы с цифровыми данными естественно использовать $p = 2$ в качестве характеристики поля. При $m = 1$ элементом кодовой последовательности будет бит, при $m = 8$ – 8 бит, т.е. байт. Собственно коды Рида–Соломона, работающие с байтами, и являются наиболее распространенными, но так как операции в конечном поле $GF(2^8)$ слишком сложны для понимания, то в этой работе используются операции в поле $GF(2^3)$.

Разработан программный модуль, который позволяет максимально доступно и наглядно показать студентам алгоритмы процессы, происходящие при формировании сигналов в кодере и обработке в декодере.

В данной программе представлен кодер Рида–Соломона(7,3) работающий с конечным полем $GF(2^3)$. Это означает, что для формирования одного блока закодированной последовательности используются три информационных символа и четыре проверочных, каждый символ состоит из трёх бит, следовательно, все возможные значения символов: 000, 010, 001, 110, 011, 111, 101, 100. Кодирование производится по систематическому методу, путём выполнения деления полинома информационных символов на образующий полином в конечном поле, операция выполняется по модулю. Остаток от деления полиномов представляет собой проверочные символы, которые припи-

ссылаются к информационным символам. В результате операции получается блок из 7 символов каждый символ, которого представляет собой трёхзначное двоичное число.

Интерфейс окна программы представлен на рис. 1.

Рис. 1. Интерфейс окна программы

Пользователем вводится сообщение, после чего программа переводит сообщение в цифровой вид согласно таблицам Unicode. Последовательности двоичных символов разделяется по 3 бита, так формируются информационные символы, и кодируются кодом Рида–Соломона (7,3). Результаты этих операций выводятся в последней строке окна программы.

На следующем этапе будет доработан декодер с учётом влияния ошибок возникающих в канале передачи информации. Программа будет вносить заданное количество ошибок в сообщение, на выходе будет наглядно представлены последствия их возникновения.

Декодер последовательно будет выполнять следующие действия:

- вычислять синдром ошибки,
- строить полином ошибки (алгоритм Берлекэмпа–Мессе).
- находить корни данного полинома (процедура Ченя),
- определять характер ошибки (метод Форни),
- исправляет ошибки.

В дальнейшем планируется создание модулей для исследования более сложных кодов и сигнально кодовых конструкций, основанных на них, с целью визуализации процессов, происходящих при кодировании и декодировании.

ЛИТЕРАТУРА

1. Гомцяц О.А. Модели и методы каскадных кодирующих конструкций и модуляции в цифровых системах обработки информации: диссертация. – Ереван, 2016. – 284 с.

2. Клейко Д.В., Лямин Н.В. Упрощение кодера Рида–Соломона при использовании альтернативных простых полиномов, образующих расширения полей Галуа. – Новосибирск, 2010. – 6 с.
3. Уэльдон Э. Коды, исправляющие ошибки: учеб. пособие. – 1976. – 283 с.
4. Википедия: код Рида–Соломона [Электронный ресурс]. – Режим доступа: <https://ru.wikipedia.org>
5. Простой пример реализации кода Рида–Соломона [Электронный ресурс]. – Режим доступа: <https://habrahabr.ru>
6. Кодирование информации с применением кода Рида–Соломона [Электронный ресурс]. – Режим доступа: <http://vbond.kiev.ua/ru>
7. Коды Рида–Соломона [Электронный ресурс]. – Режим доступа: <http://sernam.ru>
8. Аппаратная реализация кодов Рида–Соломона [Электронный ресурс]. – Режим доступа: <http://ea.donntu.org>
9. Арифметика полей Галуа для кодирования информации кодами Рида–Соломона [Электронный ресурс]. – Режим доступа: <https://sohabr.net>

МОДЕЛЬ АДАПТИВНОЙ ДВУСТОРОННЕЙ ШИРОКОПОЛОСНОЙ СПУТНИКОВОЙ СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ

А.С. Храмов, студент 5 курса

*Научный руководитель А.М. Голиков, доцент каф. РТС, к.т.н., ст.н.с.,
г. Томск, ТУСУР, каф. РТС, rts2_golikov@mail.ru*

Модель построена на стандарте цифровой видео передачи – системы с обратным каналом (Digital Video Broadcast – Return Channel System DVB-RCS), мультисервисная DVB-RCS платформа обеспечивает высокоскоростной спутниковый доступ с приложениями реального времени (передача данных, голос, видео), а также стандартные IP приложения. Нисходящая линия связи DVB-RCS построена на стандарте телевизионного вещания DVB-S2, а восходящая на стандарте MF-TDMA. В докладе представлены результаты исследования Simulink моделей DVB-S2 и MF-TDMA для использовании двух входных последовательностей. Модель будет использована для проектирования адаптивной двусторонней широкополосной спутниковой системы передачи данных для малых космических аппаратов МКА.

Топология сети на базе мультисервисной DVB-RCS платформы, как правило, строится по типу «звезда» и подразумевает наличие двух трактов передачи [1]. Прямой канал – спутниковый канал от Центральной земной станции (ЦЗС/HUB) до удаленных спутниковых интерактивных терминалов (СИТ/SIT). Обратный канал – спутниковый канал от терминала до Центральной земной станции.

Стандарт DVB-RCS утвержден Европейским институтом стандартизации в области связи (ETSI) в 2000 г. Стандарт предлагает прямой канал, основанный на формате данных DVB/MPEG 2, и обратный канал, на основе режима множественного доступа с разделением по времени (MF-TDMA). Широкополосная несущая DVB/MPEG 2 может обеспечить скорость передачи в прямом канале до 110 Мбит/с, а режим MF-TDMA предусматривает скорость до 2–4 Мбит/с в обратном канале с каждого удаленного терминала.

Стандарт DVB-S2 (прямой канал) предусматривает четыре возможных схемы модуляции.

По сравнению с QPSK, верхняя схема модуляции, 32 APSK, позволяет повысить общую скорость потока в 2,5 раза. Для защиты от помех в новом стандарте, как и в прежних, используется перемежение данных и наложение двухуровневого кода для прямой коррекции ошибок (Forward Error Correction FEC). Но системы внешней и внутренней кодовой защиты – другие, чем в стандарте DVB-S. В качестве внешней кодовой защиты вместо кода Рида–Соломона используется код Боуза–Чоудхури–Хоквингема (Bose–Bhaudhuri–Hocquenghem, BCH), а в качестве внутренней, вместо сверхточного кода, – код с низкой плотностью проверок на четность (Low Density Parity Check Codes – LDPC). Критерием выбора была достижимая с помощью кода эффективность передачи в канале, и коду LDPC удалось максимально приблизить ее к пределу Шеннона при соблюдении установленных ограничений на сложность чипа декодера. Код LDPC накладывается на блоки длиной 64800 бит, которые для приложений, чувствительных к задержкам, могут быть сокращены в 4 раза. Относительная скорость передачи может составлять от 1/4, до 9/10. Первый вариант предусматривает передачу трех защитных бит на каждый полезный, а последний, одиннадцати – один контрольный бит на девять полезных.

Новая пара кодов обеспечивают более эффективное использование канального ресурса, чем коды DVB-S. Она позволяет работать при уровнях SNR всего на 0.7 дБ выше требуемого соотношением Шеннона для заданной скорости, в то время как применение свертки в паре с кодом Рида–Соломона требовало превышения этого предела примерно на 5 дБ. Правда, при этом не выполняются условия бесконечно высокой достоверности передаваемой информации, оговоренные в теореме Шеннона. Более того, новый стандарт допускает более высокую частоту ошибок BER на выходе декодера, чем старый. Если кодеры стандарта DVB-S обеспечивают снижение BER до 10^{-10} – 10^{-11} , то LDPC в сочетании с BCH снижают его до уровня 10^{-7} . Такой уровень соответствует появлению одной ошибки в час при пе-

редаче потока скоростью 5 Мбит/с. В случае передачи пакетной информации, перед ее подачей в FEC-кодеры, на нее накладывается CRC-8 (Cyclic Redundancy Check) кодирование. А после FEC кодирования данные подвергаются перемежению, защищающему ее от длительных помех.

Реализация модели DVB-S2 (линии «вниз»).

Разработана модель в среде разработки Simulink для стандарта DVB-S2 [2].

Результаты исследования Simulink модели DVB-S2.

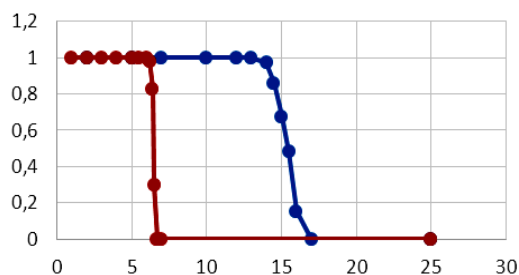


Рис. 1. График зависимости BER от SNR на входе/выходе системы. Синяя линия – для QPSK, красная линия – для 8-PSK

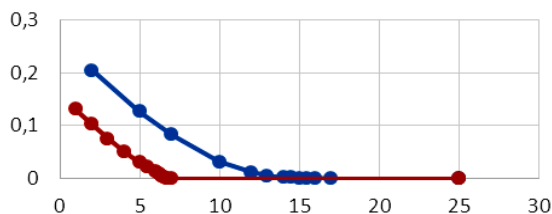


Рис. 2. График зависимости BER от SNR на LDPC-коде/декоде. Синяя линия – для QPSK, красная линия – для 8-PSK

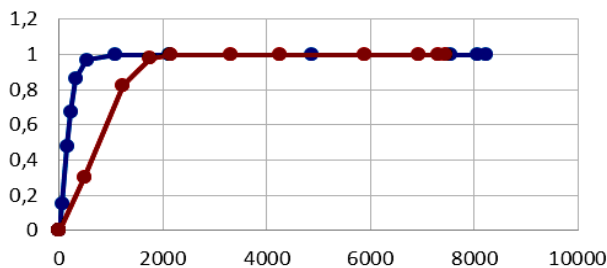


Рис. 3. График зависимости BER от контрольной суммы на входе/выходе системы. Синяя линия – для QPSK, красная линия – для 8-PSK

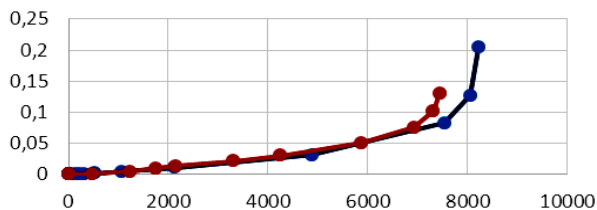


Рис. 4. График зависимости BER от контрольной суммы на LDCP-коде/декоде. Синяя линия – для QPSK, красная линия – для 8-PSK

Результаты исследований модели Symulink линии «вверх» MF-TDMA при использовании двух входных последовательностей представлены на рис.е 5. По полученным данным построены зависимости BER от SNR для первой и второй последовательности.

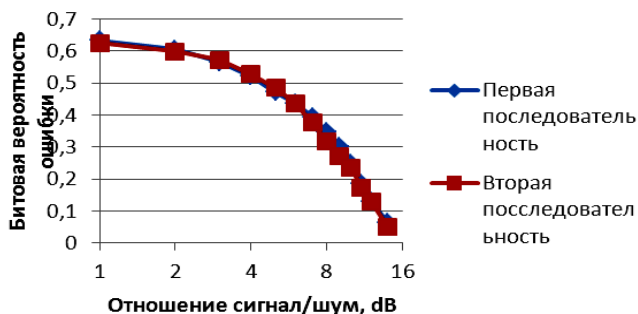


Рис. 5. Зависимость BER от SNR для двух последовательностей

В докладе представлены основные результаты исследований модели спутниковой системы передачи данных на базе стандарта DVB-RCS.

ЛИТЕРАТУРА

1. Дворкович В.П., Дворкович А.В. Видеоинформационные системы. Теория и практика. – М.: Техносфера. – 1008 с.
2. Спутниковые и телекоммуникационные системы [Электронный ресурс]. – Режим доступа: <http://www.telecomnetworks.ru/support/discription/dvbrcs/> (дата обращения 25.02.2017).

РАЗРАБОТКА СИСТЕМЫ РАДИОСВЯЗИ ПОВЫШЕННОЙ ДАЛЬНОСТИ ДЕЙСТВИЯ ДЛЯ БПЛА SUPERCAM-350

П.А. Иванов, студент 5 курса

Научный руководитель А.М. Голиков, доцент каф. РТС, к.т.н., ст.н.с.

г. Томск, ТУСУР, каф. РТС, rts2_golikov@mail.ru

*Проект ГПО РТС-1507 «Разработка моделей и имитаторов
защищенных систем спутниковой связи»*

Беспилотный летательный аппарат БПЛА Supercam-350 предназначен для выполнения панорамной и плановой аэрофотосъемки и видеосъемки, а также для других похожих задач. В настоящее время БПЛА Supercam-350 оснащен системой радиосвязи с дальностью действия до 70 км. В данной работе предложено использовать систему связи на базе стандарта IEEE 802.16m. Стандарт IEEE 802.16 m позволяет увеличить дальность системы радиосвязи БПЛА Supercam-350 и организовать Mesh-сеть для «роя» БПЛА.



Рис. 1. Supercam-350

В работе исследована Simulink модель стандарта IEEE 802.16, получены зависимости BER от SNR для отдельных видов модуляции и скорости кодирования.

Мобильные системы связи на базе стандарта IEEE 802.16 ориентированы на работу с пользователями, передвигающимися со скоростью до 150 км/ч, дальностью действия до 200 км (в условиях прямой видимости), скоростью передачи информации 600 Мбит/с (при использовании технологии MIMO).

В каждый момент времени, используемый вид модуляции и скорость кодирования (R) адаптируются под условия передачи. Блок «Adaptive Rate Control» анализирует уровень SNR в приемном устройстве и устанавливает параметры в соответствии с таблицей.

Система адаптируется к условиям передачи, изменяя вид сигнально-кодовой конструкции сигнала (табл.). Созвездие принимаемого сигнала отображены на рис. 3, 4.

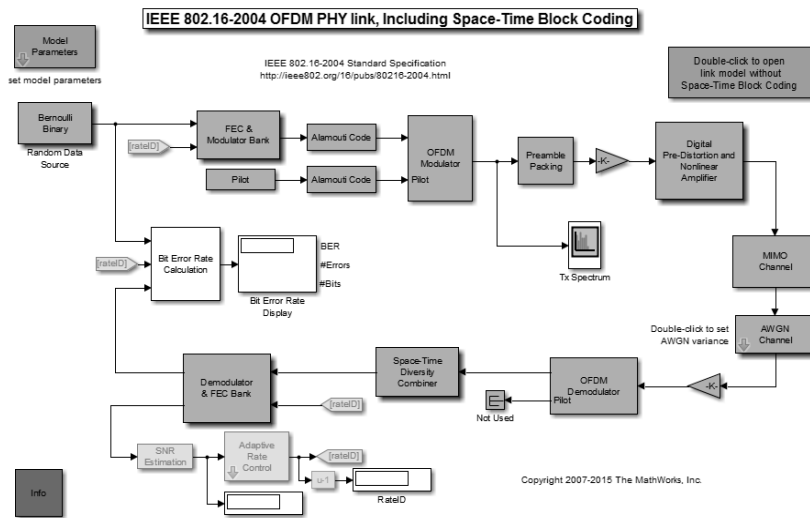


Рис. 2. Модель IEEE 802.16 в MATLAB 2015b

Изменение параметров модуляции и кодирования в зависимости от SNR

Вид модуляции и скорость кодирования	Отношение сигнал/шум в приемнике, дБ
BPSK	$\text{SNR} < 4$
QPSK, $R=1/2$	$4 \text{ дБ} < \text{SNR} < 10$
QPSK, $R=3/4$	$10 \text{ дБ} < \text{SNR} < 12$
16-QAM, $R=1/2$	$12 \text{ дБ} < \text{SNR} < 19$
16-QAM, $R=3/4$	$19 \text{ дБ} < \text{SNR} < 22$
64-QAM, $R=1/2$	$22 \text{ дБ} < \text{SNR} < 28$
64-QAM, $R=3/4$	$\text{SNR} > 28$

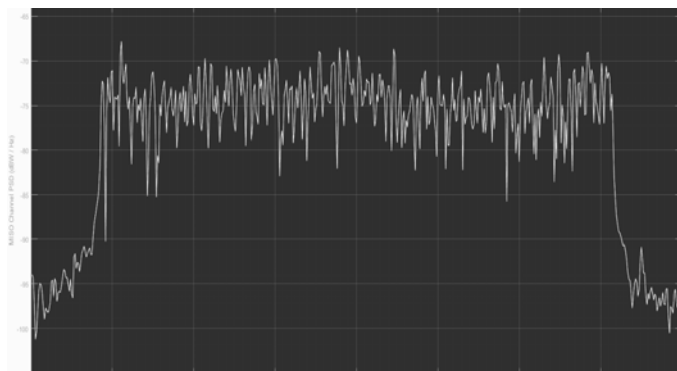


Рис. 3. Спектр принимаемого сигнала

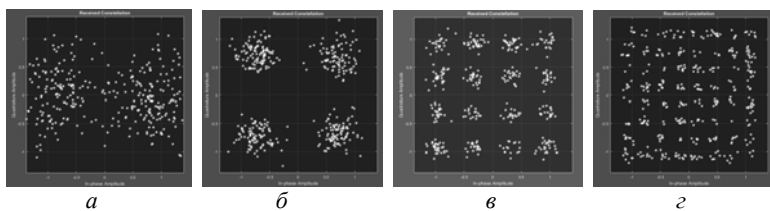


Рис. 4. Созвездие принимаемого сигнала:
 a – SNR = 2; $б$ – SNR = 11; $в$ – SNR = 18; $г$ – SNR = 22

В результате моделирования получены зависимости битовой вероятности ошибки (BER) от отношения сигнал/шум (SNR).

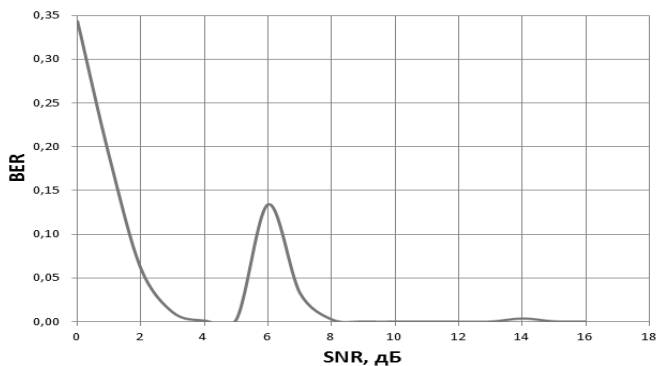


Рис. 5. Зависимость BER от SNR при использовании адаптивного изменения параметров

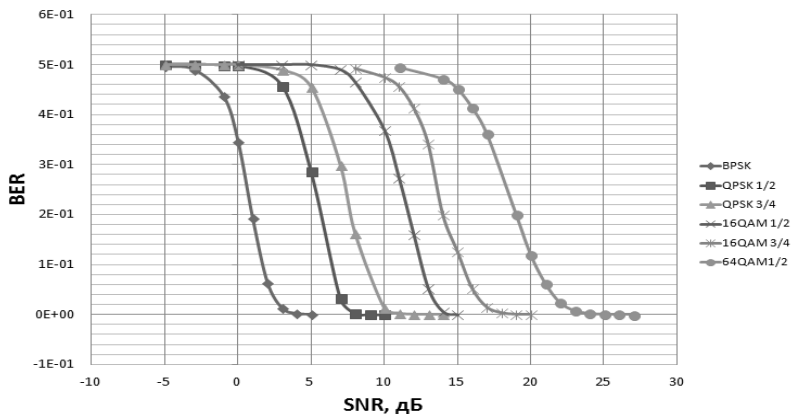


Рис. 6. Графики зависимости BER от SNR для отдельных видов модуляции и скорости кодирования

В данной работе предложено использовать систему связи на базе стандарта IEEE 802.16m. Стандарт IEEE 802.16m позволяет увеличить дальность системы радиосвязи БПЛА Supercam-350 и организовать Mesh-сеть для «роя» БПЛА. Предложенная система радиосвязи для БПЛА Supercam-350 обеспечит его дальность действия до 200 км (в условиях прямой видимости) со скоростью передачи данных 600 Мбит/с (при использовании технологии MIMO, а также позволит организовать Mesh-сеть для «роя» БПЛА.

ЛИТЕРАТУРА

1. Боев Н.М. Адаптивное изменение параметров цифровых систем связи комплексов беспилотных летательных аппаратов // 22-я Междунар. Крым. конф. «СВЧ-техника и телекоммуникационные технологии», 10–14 сент., 2012 г.: Материалы конф.: в 2 т. – Т. 1.

СИСТЕМА МОБИЛЬНОЙ СВЯЗИ ДЛЯ АНПА «ГЛАЙДЕР» НА БАЗЕ ГРУППИРОВКИ НИЗКООРБИТАЛЬНЫХ СПУТНИКОВ «ГОНЕЦ-Д1М»

К.Д. Карпачев, студент 4 курса

*Научный руководитель А.М. Голиков, доцент каф. РТС, к.т.н., с.н.с.,
г. Томск, ТУСУР, каф. РТС. rts2_golikov@mail.ru*

Спутниковые системы связи зачастую являются единственно возможным видом связи в случае предоставления услуг в труднодоступных и удаленных регионах, например, в арктических морях. Кроме того, спутниковые системы связи обладают таким качеством, как возможность передачи одной и той же информации неограниченному кругу пользователей, находящихся в зоне видимости спутника ретранслятора.

Технические характеристики автономных необитаемых подводных аппаратов (АНПА) «Глайдеров»:

- 1) длина 3000 мм (без хвостовой антенны);
- 2) диаметр (без крыльев) 310 мм;
- 3) размах горизонтального оперения 1370 см;
- 4) масса 150 кг;
- 5) скорость 1 – 2 узла;
- 6) максимальная автономность: 6 мес.;
- 7) все полезной нагрузки: до 15 кг;
- 8) система управления: дистанционная по радиоканалу, автономная.



Рис. 1. АНПА «Глайдер»

Многофункциональная система персональной спутниковой связи «Гонец-Д1М» (МСПСС) представляет собой систему связи на основе орбитальной группировки, состоящей из 24 спутников гражданского назначения «Гонец-М1». Также предоставляет следующие услуги:

- накопление и сброс информации: данные с абонентских терминалов собираются, обрабатываются, накапливаются и по запросу передаются конечному пользователю;

- обмен короткими сообщениями: сообщения АТ собираются, обрабатываются, накапливаются и передаются на другой АТ внутри системы «Гонец-Д1М», или во внешнюю наземную сеть;

- передача данных: данные с абонентских терминалов собираются, обрабатываются, накапливаются и передаются на другой АТ внутри системы «Гонец-Д1М», или во внешнюю наземную сеть;

- голосовая связь: мобильные АТ получают доступ к другому АТ (точка-точка), находящемуся в зоне обслуживания того же КА, или к внешним наземным телефонным линиям (таблица).

Основные тактико-технические характеристики спутниковой системы связи «Гонец-Д1М»

Характеристика	Значение	
Скорость передачи информационных данных до кодирования и модуляции	Линия вверх	Линия вниз
	1024 кбит/с	2048 кбит/с
Частота	5150 ÷ 5205 МГц	6700÷7075 МГц
BER	10^{-7}	
Дальность связи	Каждый из 24-х КА покрывает зону с диаметром около 5800 км	

Время покрытия в процентном выражении (рис. 2–4) показаны точки сетки (широта/долгота $1 \times 1^\circ$), составляющей зону покрытия, для которой указано время покрытия в процентном выражении относительно 24 ч, когда зона покрывается, как минимум, одним спутником,

при угле места не менее 10° . Диапазоны времени покрытия в процентном выражении всегда больше 90%, за исключением ограниченного количества площадок, для которых время видимости (при угле места не менее 10°) немного менее 90% (~88%). Если рассматривать только территорию Российской Федерации, то для нее время покрытия всегда больше 90%.

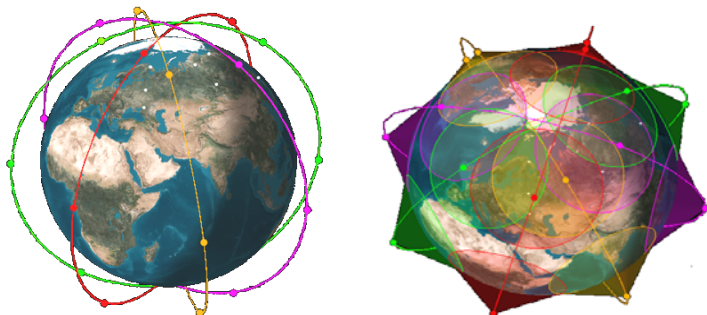


Рис. 2. Низкоорбитальная спутниковая группировка «Гонец-Д1М»

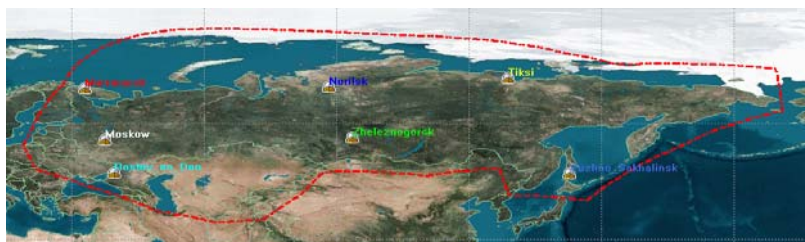


Рис. 3. Зона покрытия и региональные станции

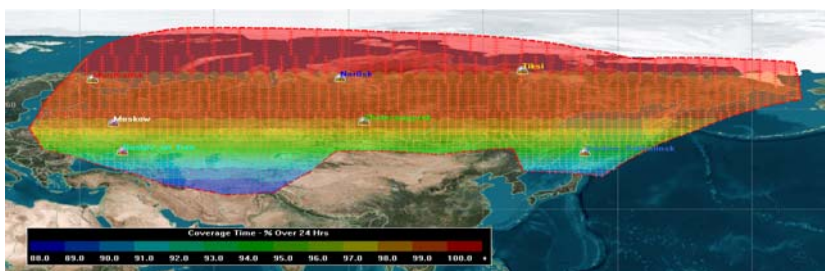


Рис. 4. Время покрытия в процентном выражении относительно 24 часов

Сигнально-кодовая конструкция системы связи включает сверточный кодер (декодер Витерби), кодер Рид-Соломона и модулятор (BPSK, QPSK, 16-QAM, 64-QAM). Зависимость вероятности битовой ошибки (BER) от отношения сигнал / шум (SNR) дана на рис. 5.

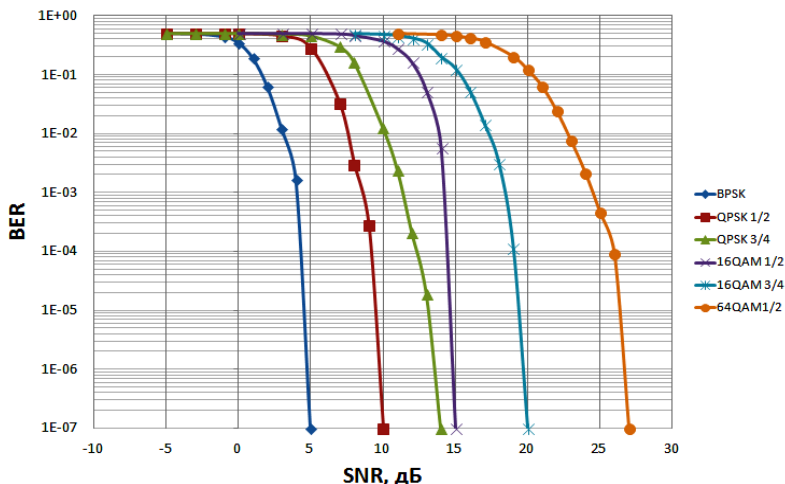


Рис. 5. Зависимость BER от SNR, для BPSK-, QPSK-, 16-QAM-, 64-QAM-модуляции, при скорости кода 1/2, 2/3, 3/4, 5/6

В работе показано, что для организации передачи данных с АНПА «Глайдеров» может быть использована система персональной спутниковой связи «Гонец-Д1М», обеспечивающая до 90% времени в сутки передачи данных для арктических широт работы АНПА «Глайдеров» со скоростью 2 МБ/сек и $BER = 10^{-7}$.

ЛИТЕРАТУРА

1. Сомов А.М., Корнев С.Ф. Спутниковые системы связи: учеб. пособие для вузов / Под ред. А.М. Сомова. – М.: Горячая линия–Телеком, 2012. – 244 с.
2. Гонец (спутниковая система связи) [электронный ресурс]. – Режим доступа: [http://ru.wikipedia.org/wiki/Гонец_\(спутниковая_система_связи\)](http://ru.wikipedia.org/wiki/Гонец_(спутниковая_система_связи)) (дата обращения: 25.01.2014).

СИСТЕМА НЕЙРОСЕТЕВОЙ ОБРАБОТКИ ИЗОБРАЖЕНИЙ РЕЧНОГО РАДИОЛОКАТОРА

Д.В. Дудкин, М.Д. Медведев, студенты

Научный руководитель А.М. Голиков, доцент каф. РТС, к.т.н., с.н.с.,

г. Томск, ТУСУР, каф. РТС, rts2_golikov@mail.ru

«Проект ГПО РТС–1602 «Разработка перспективных методов обработки сигналов и изображений радиолокационных станций»

При помощи совместной системы вейвлет фильтрации сигналов и нейросетевой обработки изображений радиолокатора можно увели-

чить качество и четкость отображения объектов на индикаторе радиолокационной станции, увеличить максимальную дальность обнаружения и распознавания малоразмерных объектов. Так же можно внедрить эту систему в РЛС «Река» научно-производственной фирмы МИКРАН [2].

Радиолокационные изображения РЛС «Река» до и после нейросетевой обработки даны на рис. 1, 2.

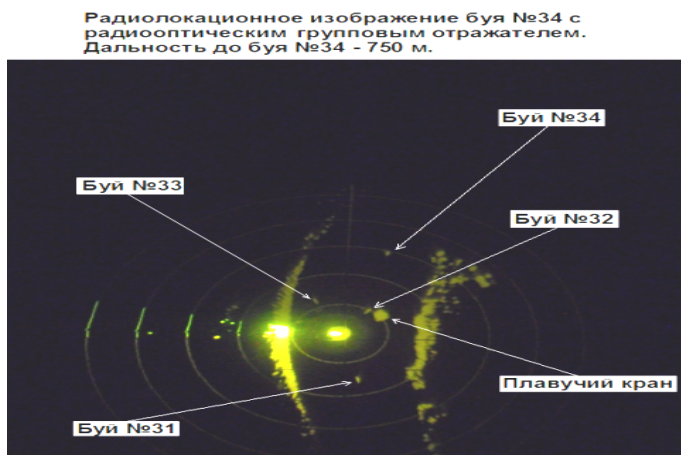


Рис. 1. Изображение РЛС «Река» до обработки

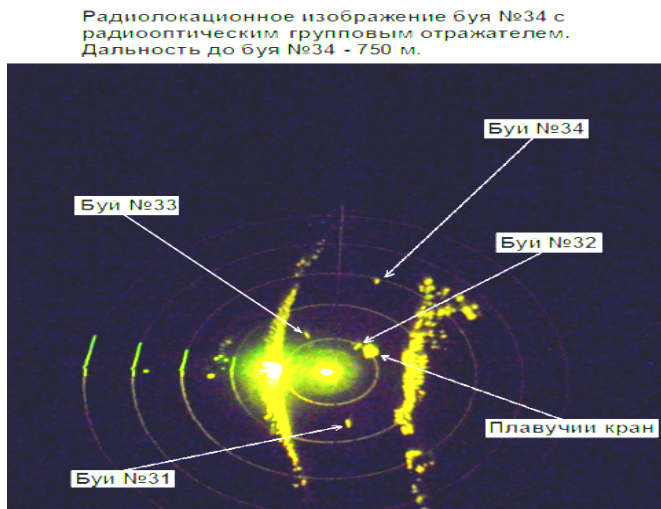


Рис. 2. Результаты обработки трехэтапным методом

Трехэтапный метод обработки:

1 этап. Предобработка.

Данный этап включает в себя мультипликативную подстройку яркости исходного изображения

2 этап. Локальная обработка с помощью искусственной нейронной сети.

3 этап. Автонастройка уровней.

Алгоритм автоматической настройки уровней яркости заслуживает внимание благодаря своему качеству и скорости работы. Согласно этому алгоритму, каждый цветовой канал изображения обрабатывается отдельно [3].

Совместная вейвлет-фильтрация сигнала и нейронная обработка изображения РЛС после фильтрации позволяет улучшить технические характеристики радара [1].

Обработке подверглось 200 измерений разности дальностей (до и после нейронной обработки) и для лучшего восприятия данных, была построена гистограмма (распределение) разностей дальностей, где по оси OX отложены равные промежутки по дальности ΔR , по оси OY – распределение вероятностей в % (рис. 3).

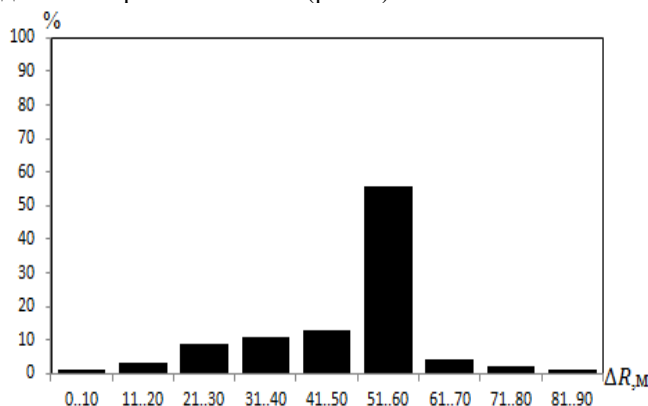


Рис. 3. Гистограмма результатов измерений разности дальностей обнаружения с нейросетевой обработкой и без нее

Гистограмма показывает, что после нейронной обработки изображений РЛС, дальность обнаружения, в среднем, увеличивается на 55 м.

Был предложен трехэтапный метод быстрой нейронной обработки цифровых изображений. Этот способ позволяет улучшить обработку изображений. Сравнение трехэтапной обработки изображений (предобработка + НС + автонастройка уровней) с рядом существующих

ших подходов показало ее применимость для повышения качества изображений, но только при обработке изображений ландшафтов Земной поверхности.

Была поставлена задача достичь максимального улучшения качества изображения на индикаторе РЛС, путем использования совместной системы вейвлет-фильтрации сигнала и нейронной обработки изображения, что должно привести к увеличению максимальной дальности обнаружения и улучшению разрешающей (по углу) способности РЛС.

Рассмотрен по пиксельный метод обработки изображений, который является лучшим среди представленных. Проведя испытания по дальности обнаружения, можно подвести итог, что по пиксельная обработка изображений на много лучше трехэтапной. Исходя из гистограммы видно, что после обработки дальность обнаружения, в среднем, увеличилась на 55 метров.

ЛИТЕРАТУРА

1. Микран [Электронный ресурс]. – Режим доступа: <http://www.micran.ru/> (дата обращения: 20.11.2016).
2. Уэлетид С. Фракталы и вейвлеты для сжатия изображений в действии: учеб. пособ. – М.: Триумф, 2003 – 320 с.
3. Головкин В.А. Нейроинтеллект: Теория и применения. – Кн. 1. Организация и обучение нейронных сетей с прямыми и обратными связями. – Брест: БПИ, 1999. – 260 с.

МОДЕЛЬ СИСТЕМЫ МОБИЛЬНОЙ СВЯЗИ СТАНДАРТА IEEE 802.16 (WiMAX) НА БАЗЕ ПО МАТЛАВ

А.В. Кригер, студент

*Научный руководитель А.М. Голиков, доцент каф. РТС, к.т.н., с.н.с.
г. Томск, ТУСУР, каф. РЗИ, rts2_golikov@mail.ru*

Под аббревиатурой WiMAX (Worldwide Interoperability for Microwave Access) понимается технология операторского класса с высоким качеством сервиса, которая основана на семействе стандартов IEEE 802.16, разработанных международным институтом инженеров по электротехнике и электронике (IEEE). Обеспечивает мульти-сервисность, гибкое распределение частот, задание приоритетов различным видам трафика, возможность обеспечения разного уровня качества (QoS), поддержка интерфейсов IP. Эта технология позволяет параллельно передавать голос, мультимедийную информацию и цифровые данные по одному каналу связи. Важным преимуществом явля-

ется возможность быстро наращивать емкость и расширять территорию связи.

Модель IEEE 802.16 в MATLAB 2015b представлена на рис. 1.

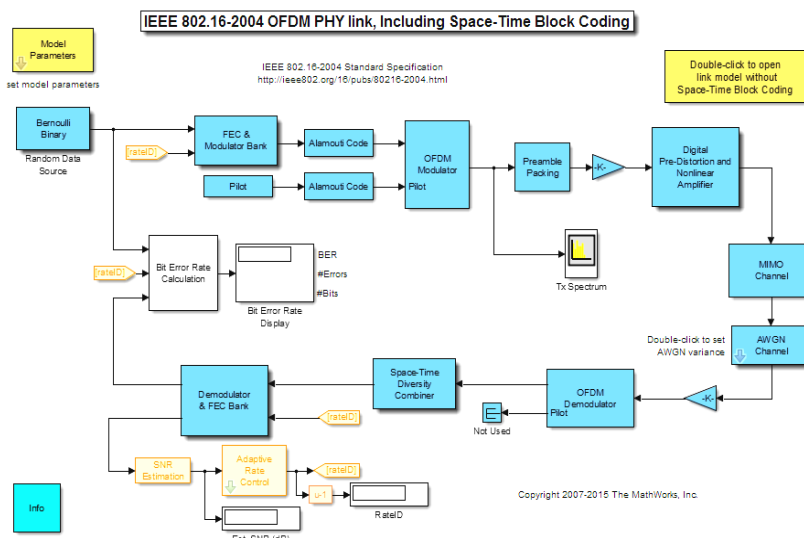


Рис. 1. Модель IEEE 802.16–2004 OFDM в MATLAB 2015b

Система IEEE 802.16 является широкополосной и адаптивной и использует сигнально-кодовые конструкции от сверточного кода и модулятора BPSK (рис. 2) до кода Рида–Соломона, сверточного кода и модулятора 64QAM 3/4 (рис. 3).

Состав блока модулятора BPSK 1/2:

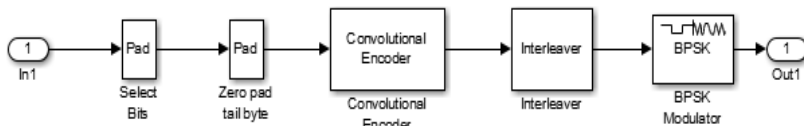


Рис. 2. Состав блока модулятора «BPSK 1/2»

Состав блока модулятора 64QAM 3/4:

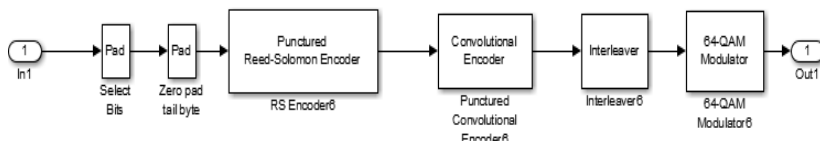


Рис. 3. Состав блока модулятора «64QAM 3/4»

Блок помехоустойчивого кодирования и модуляции («FEC & Modulator Bank», рис. 4) производит формирование сигнально-кодовой конструкции (СКК) определенного вида в зависимости от условий передачи.

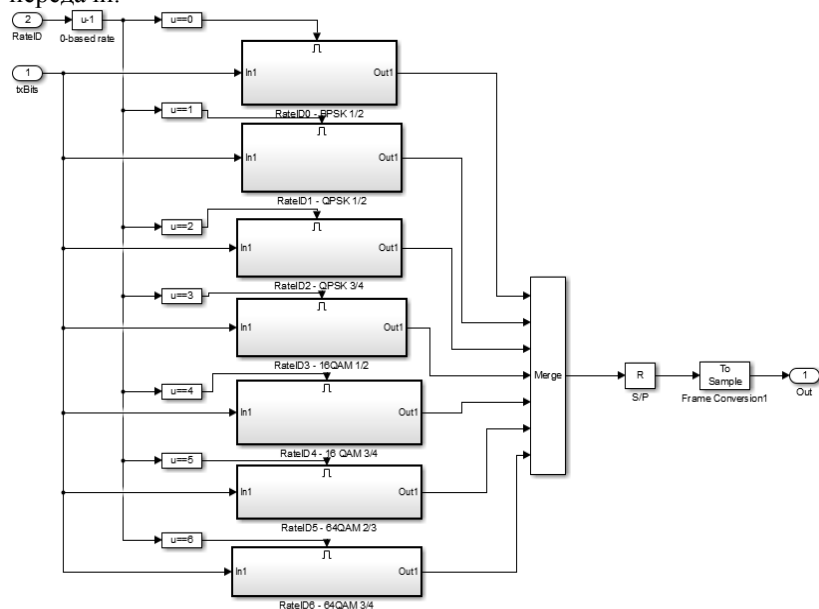


Рис. 4. Состав блока «FEC & Modulator Bank»

Формирование сигнально-кодовых конструкций в каждом блоке происходит следующим образом: к поступающим информационным битам добавляется определяется «хвост» из нулевых бит, полученная последовательность кодируется блочным циклическим кодом Рида-Соломона. Следующий этап кодирования – сверточный код с использованием Треллис-структуры, затем, после перемежения, последовательность бит модулируется определенным образом для передачи по каналу.

Вид модуляции и скорость кодирования	Отношение сигнал/шум в прием- нике, дБ
BPSK	$SNR < 4$
QPSK, $R=1/2$	$4 < SNR < 10$
QPSK, $R=3/4$	$10 < SNR < 12$
16-QAM, $R=1/2$	$12 < SNR < 19$
16-QAM, $R=3/4$	$19 < SNR < 22$
64-QAM, $R=1/2$	$22 < SNR < 28$
64-QAM, $R=3/4$	$SNR > 28$ дБ

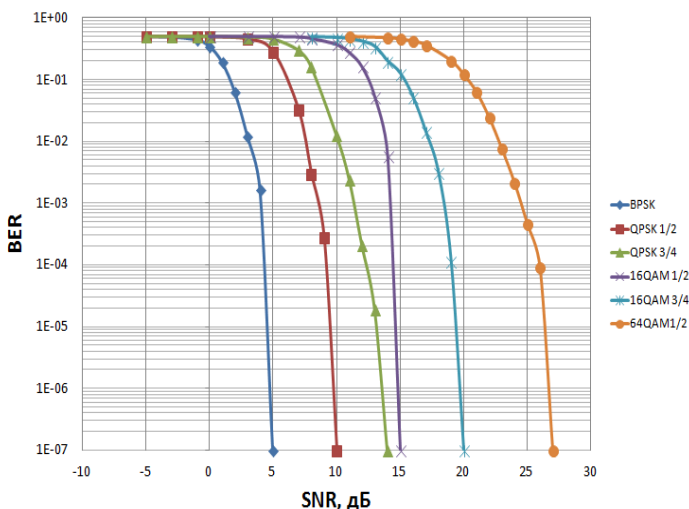


Рис. 5. Графики зависимости BER от SNR для отдельных видов модуляции и скорости кодирования. Логарифмическая шкала

По результатам практического исследования модели физического уровня IEEE 802.16–2004 показано, что адаптивное изменение параметров системы в зависимости от SNR в канале приводит к уменьшению вероятности ошибок.

ЛИТЕРАТУРА

1. Технология беспроводного доступа WiMAX [Электронный ресурс]. – Режим доступа: <http://systemseti.com> (дата обращения: 15.10.2017).
2. Вишневский В.М., Портной С.Л., Шахнович И.В. Энциклопедия WiMAX. Путь к 4G. – М.: Техносфера, 2009. – 472 с.

СИСТЕМА ПЕРЕДАЧИ ДАННЫХ САМООРГАНИЗУЮЩЕЙСЯ СЕТИ БАЛЛИСТИЧЕСКИ СВЯЗАННОЙ ГРУППЫ МАЛЫХ КОСМИЧЕСКИХ АППАРАТОВ НА БАЗЕ СТАНДАРТА IEEE 802.16M

А.С. Кудряшов, студент 5 курса

*Научный руководитель А.М. Голиков, доцент каф. РТС, к.т.н., с.н.с.
г. Томск, ТУСУР, каф. РТС, rts2_golikov@mail.ru*

*Проект ГПО «РТС–1507 Разработка моделей и имитаторов
защищенных систем спутниковой связи»*

В данной работе рассмотрена возможность создания система передачи информации для баллистически связанной группы космиче-

ских аппаратов дистанционного зондирования земли «Ресурс-П» на базе стандарта IEEE 802.16m. Баллистически связанная группа МКА – совокупность из нескольких космических аппаратов, движущихся на сравнительно близком взаимном расстоянии от несколько десятков метров до сотни километров.

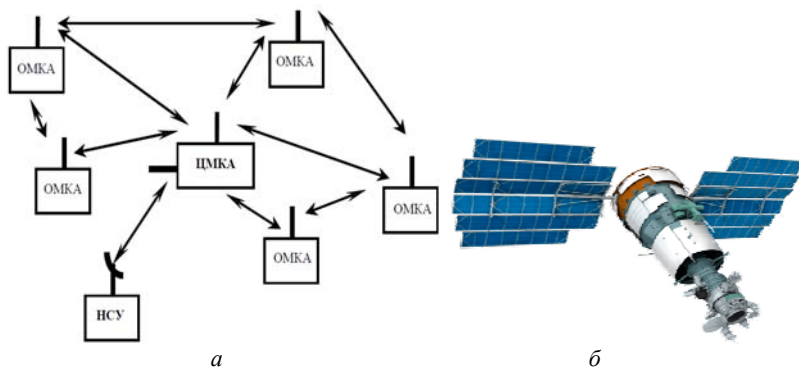


Рис. 1. Организация беспроводной сети передачи данных между МКА – *а*; внешний вид аппарата «Ресурс-П» – *б*; (ЦМКА – центральный МКА, ОМКА – оконечный МКА, НСУ – наземная станция управления)

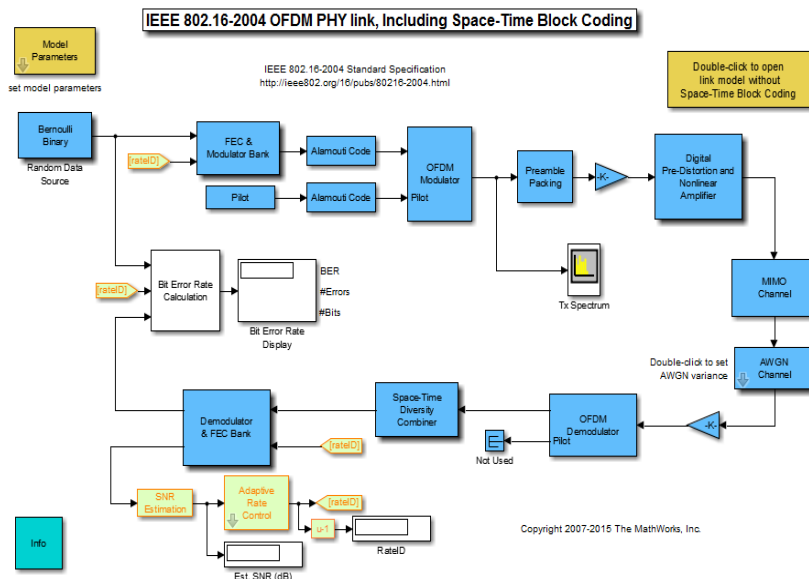


Рис. 3. Схема системы WiMAX в Simulink

Управление осуществляется с учётом взаимного положения спутников, движущихся по весьма близким орбитам, т.е. реализуется управление относительным движением.

Основным достоинством IEEE 802.16m является увеличенная скорость передачи данных (до 100 Мбит/с при использовании mobile WMAN). Для увеличения пропускной способности в стандарте закреплены такие нововведения, как многоканальный прием и передача данных (MIMO). Применяемая в стандарте IEEE 802.16m технология mesh network дает возможность автоматического конфигурирования и восстановления сети: система сама определяет наиболее оптимальный путь для передачи сигнала и производит переконфигурирование этого пути в случае каких-либо сбоев.

Получены зависимости битовой вероятности ошибки от отношения сигнал/шум для различных видов модуляции и скорости кодирования.

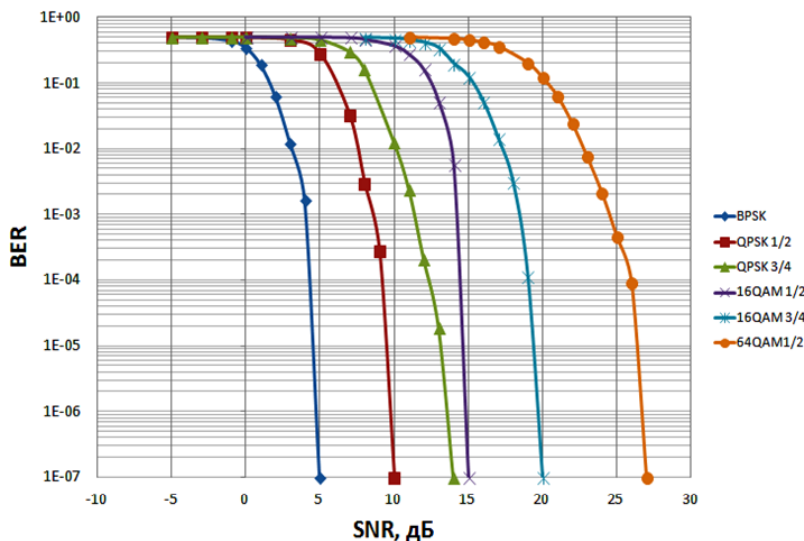


Рис. 4. Зависимости BER от SNR

При энергетическом расчете линии передачи «ЦМКА-НСУ» использовались следующие условия: высота круговой орбиты КА «Ресурс-П» составляет 475 км, IEEE 802.16m работает на частоте 1,5 ГГц, мощность передатчика составляет 5 Вт. Требуемый запас по энергетике – не менее 20 дБ. Для данных условий подобраны необходимые параметры передатчиков и антенн.

Рабочая частота	Расстояние между точками	
1500 (MHz)	475 (км)	
Мощность передатчика	Усиление антенны передатчика	Потери в кабеле и разъемах 1
37 (dBm)	5 (dBi)	1 (dB)
Чувствительность приемника	Усиление антенны приемника	Потери в кабеле и разъемах 2
-110 (dBm)	20 (dBi)	1 (dB)
Результаты расчета:		
Рассчитать запас сигнала		
Потери в свободном пространстве	Уровень сигнала на входе приемника	Запас по энергетике канала
149.5 (dB)	-89.5 (dBm)	20.5 (dB)

Рис. 5. Энергетический расчет

ЛИТЕРАТУРА

1. Бараш Л.Е. Многообразие стандартов беспроводных технологий // Компьютерное обозрение. – 2003. – С. 25–29
2. Вишневский В.М., Ляхов А.И., Портной С.Л., Шахнович И.Л. Широкополосные беспроводные сети передачи информации. – М.: Техносфера, 2005. – С. 44–57
3. Ресурс-П [Электронный ресурс]. – Режим доступа: <http://russian-spacesystems.ru/bussines/dzz/orbitalnaya-gruppirovka-ka-dzz/resurs-p/> (дата обращения: 22.02.2018).

МОДЕЛИРОВАНИЕ И ИССЛЕДОВАНИЕ ГЕНЕРАТОРА ПСЕВДОСЛУЧАЙНЫХ СИГНАЛОВ НА ОСНОВЕ НЕЛИНЕЙНЫХ ДИНАМИЧЕСКИХ СИСТЕМ ЛОРЕНЦА

В.А. Лобов, студент

*Научный руководитель В.В. Афанасьев, проф. каф. КНИТУ КАИ,
д.т.н.*

ivans8585@mail.ru, dobropozhalovat1@mail.ru

В данной статье рассматривается разработка генератора псевдослучайных сигналов на основе нелинейных динамических систем Лоренца. Системы передачи информации на основе разных режимов работы нелинейных динамических систем являются перспективным направлением развития систем связи с использованием динамического хаоса.

Проведено моделирование в среде MathLAB, так как программа имеет неограниченные возможности по сбору визуальных данных и функционалу. Целью моделирования является исследование поведения системы с учетом изменения начальных условий. Для решения дифференциальных уравнений был выбран метод Эйлера. Смоделирована система Лоренца, оценены значения дисперсии, математического ожидания и СКО сигналов генератора псевдослучайных сигналов на базе системы Лоренца при изменении начальных условий системы, изучено поведение системы, построены зависимости амплитуды колебаний от времени и сделаны выводы о реакции системы Лоренца на изменения начальных условий.

**Значения дисперсии, мат. ожидания и СКО
для разных начальных условий**

	$X(1) = 1, Y(1) = 0, Z(1) = 0$	$X(1) = 1,44, Y(1) = 2,58, Z(1) = 17,44$
$X(1)$	$D(X) = 63,3366$ $M(X) = -0,8929$ $CKO(X) = 7,9584$	$D(X) = 62,5387$ $M(X) = 0,0159$ $CKO(X) = 7,9081$
$Y(1)$	$D(Y) = 79,8235$ $M(Y) = -0,8962$ $CKO(Y) = 8,9344$	$D(Y) = 81,7996$ $M(Y) = 0,0264$ $CKO(Y) = 9,0443$
$Z(1)$	$D(Z) = 67,6207$ $M(Z) = 23,9798$ $CKO(Z) = 8,2232$	$D(Z) = 75,7352$ $M(Z) = 23,4532$ $CKO(Z) = 8,7026$

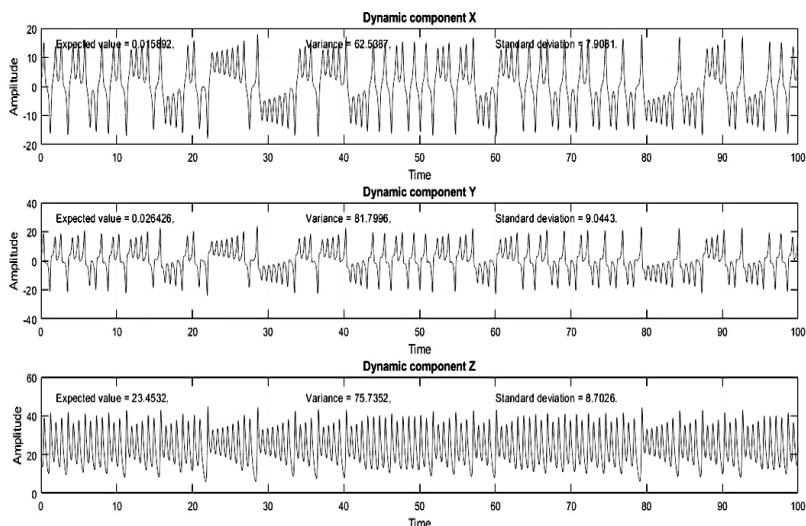


Рис. 1. Зависимость амплитуды от времени для начальных условий
 $X(1) = 1,44; Y(1) = 2,58; Z(1) = 17,44$

Исследования проводятся для обеспечения устойчивого функционирования генератора псевдослучайных сигналов на основе нелинейных динамических систем Лоренца. Таким образом, разработанная система может служить для исследования и оптимизации параметров систем с переключением хаотических режимов на базе нелинейных систем Лоренца.

ЛИТЕРАТУРА

1. Дмитриев А.С., Панас А.И. Динамический хаос: новые носители информации для систем связи. – М.: Изд-во физико-математической литературы, 2002. – 252 с.
2. Кузнецов С.П. Динамический хаос (курс лекций): учеб. пособие для вузов. – 2-е изд. перераб. и доп. – М.: Изд-во физико-математической литературы, 2006. – 356 с.
3. Аттрактор Лоренца [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Аттрактор_Лоренца (дата обращения: 15.02.18).
4. Динамическая система Лоренца и вычислительный эксперимент [Электронный ресурс]. – Режим доступа: <https://habrahabr.ru/post/229959> (дата обращения: 20.02.18).

МОДЕЛЬ МОДУЛЯТОРА APSK В LABVIEW

М.Д. Медведев и В.С. Кралинов, студенты 4 курса

*Научный руководитель А.М. Голиков, доцент каф. РТС, к.т.н., с.н.с.
г. Томск, ТУСУР, каф. РТС, rts2_golikov@mail.ru*

*Проект ГПО РТС-1602 «Разработка перспективных методов
обработки сигналов и изображений радиолокационных станций»*

Скоростные схемы модуляции 16 APSK и 32 APSK ориентированы на профессиональные системы спутникового телевидения, где часто используются слабые наземные передатчики, не вводящие бортовые ретрансляторы в нелинейный режим работы, а на приемной стороне устанавливаются профессиональные конвертеры (LNB), позволяющие с высокой точностью оценить фазу принимаемого сигнала. Эти схемы модуляции можно использовать и в системах вещания, но этом случае каналаобразующее оборудование должно поддерживать сложные варианты предискажений, а на приемной стороне должен быть обеспечен высокий уровень отношения сигнал/шум. Символы внутри констелляционного поля APSK модулированного сигнала размещены по окружностям. Такой вариант является наиболее помехоустойчивым в плане передачи амплитуды символа и позволяет использовать ретрансляторы в режимах, близких к точке насыщения.

Обратим внимание на то, что, по сравнению с QPSK, верхняя схема модуляции, 32 APSK позволяет повысить общую скорость потока в 2,5 раза.

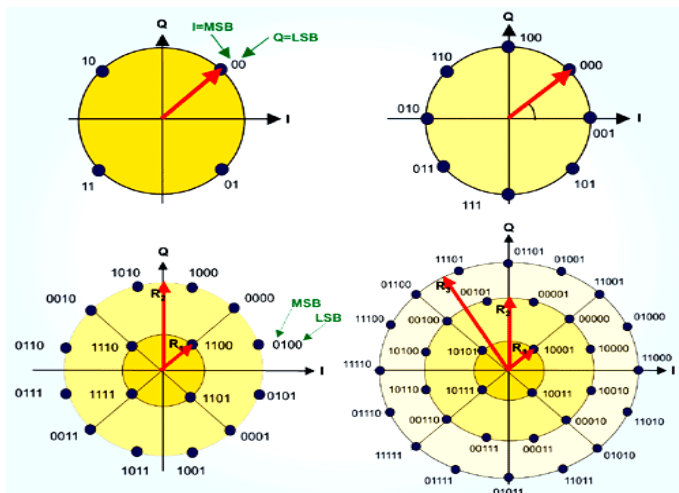


Рис. 1. Четыре схемы модуляции, применяемых в стандарте DVB-S2: QPSK, 8PSK, 16PSK, 32PSK

В работе исследуется модель модулятора на базе ПО LabVIEW.

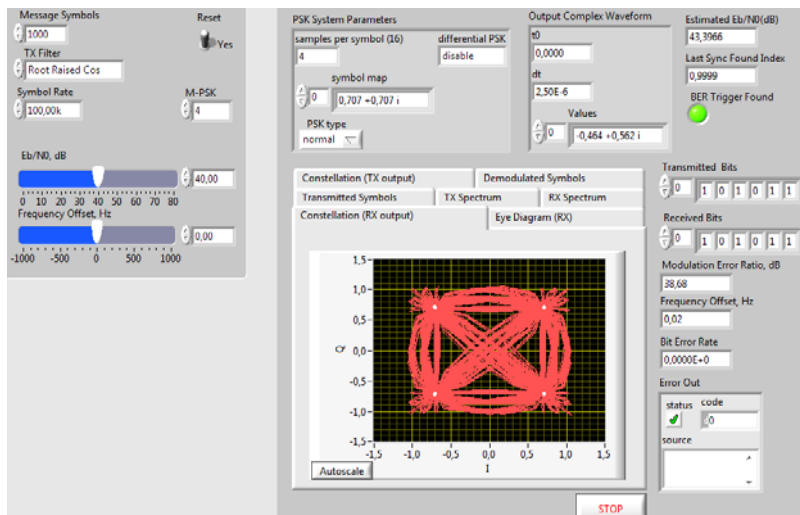


Рис. 2. Модулятор APSK в LabVIEW

Методы модуляции 16APSK и 32APSK обладают наибольшей спектральной эффективностью и приближаются к границе К. Шеннона [1].

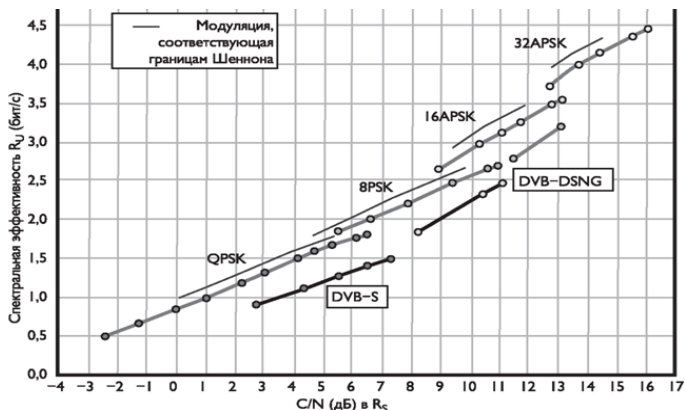


Рис. 3. Зависимость C/N от спектральной эффективности, полученная с помощью моделирования для канала с гауссовским шумом

Результаты исследования помехоустойчивости методов модуляции 16APSK и 32APSK приведены на рис. 4 [2, 3].

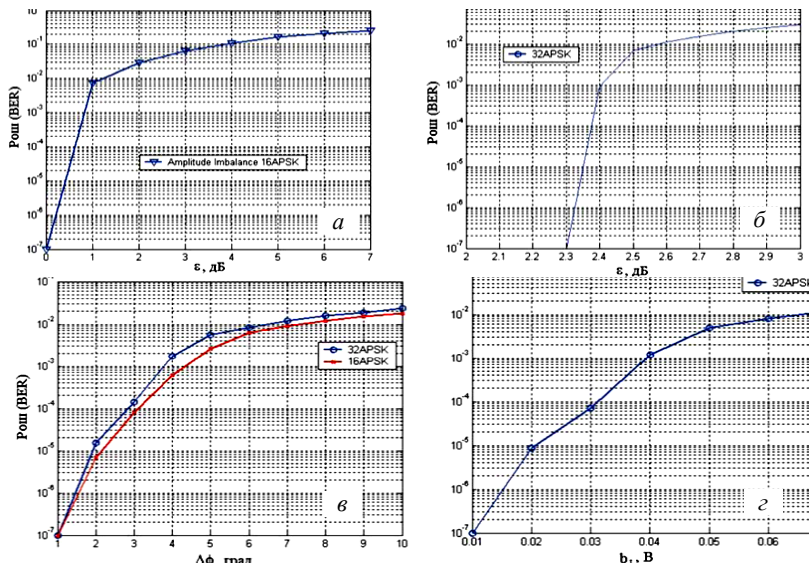


Рис. 4. Ухудшение помехоустойчивости систем стандарта DVB-S2 в зависимости от разбаланса амплитуд (а, б) фаз (в) квадратурных преобразователей, смещения постоянной составляющей (г) аналогового входного каскада. Параметры модуляции и кодирования: 16APSK R = 9/10 число итераций LDPC-кодера 50, ОСШ = 13,3 дБ; 32APSK = 9/10 число итераций LDPC-кодера 50, ОСШ = 16,2 дБ

Виды модуляции 16APSK и 32APSK отличаются высокой помехоустойчивостью и имеют большие перспективы для использования в современных системах связи.

ЛИТЕРАТУРА

1. Песков С.Н., Ищенко А.Е. Расчет вероятности ошибки в цифровых каналах связи / Теле-Спутник. – 2010. – №11. – С. 70–75.
2. Eroz M., Sun F.-W., Lec L.-N. DVB-S2 Low Density Parity Check Codes with near Shannon Limit Performance // International Journal on Satellite Communication Networks. – 2004. – Vol. 22.
3. ETSI TR 102 376 v1.1.1 (2005-02). Digital Video Broadcasting (DVB); User guidelines for the second generation system for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications (DVB-S2).

ВЕЙВЛЕТ-ФИЛЬТРАЦИЯ СИГНАЛОВ МОРСКОГО РАДИОЛОКАТОРА НА ФОНЕ ВЗВОЛНОВАННОЙ МОРСКОЙ ПОВЕРХНОСТИ

А.С. Никонов, студент

*Научный руководитель А.М. Голиков, доцент каф. РТС, к.т.н.
г. Томск, ТУСУР, каф. РТС, rts2_golikov@mail.ru*

В работе предлагается использовать вейвлет-фильтрацию сигнала по нескольким направлениям: кодирование и декодирование принимаемого изображения, с соответствующим сохранением качества и улучшением разрешающей способности графики применяемых в современных интерполяторах и аналогичными свойствами вейвлет-преобразований; использование для передачи видеоизображения современных видеоформатов, применяющих технологию вейвлет- и фрактал-преобразования.

Вейвлетное сжатие – общее название класса методов кодирования изображений, использующих двумерное вейвлет разложение кодируемого изображения или его частей. Обычно подразумевается сжатие с потерей качества. Вейвлеты дают информацию об основных пространственных и частотных характеристиках изображений, в отличие от обычного преобразование Фурье, которое выявляет лишь дает информацию о частотных характеристиках изображения.

Вейвлеты обладают рядом интересных общих свойств:

1. Разделимость, масштабируемость и переносимость.
2. Кратномасштабная совместимость
3. Ортогональность

У каждого вейвлета есть свое имя, название. (Haar, Doubechies, Coyfflets – некоторые из них) [1, 2]. Алгоритм вейвлет-обработки изо-

бражения можно свести к построению фильтров вейвлетной декомпозиции и реконструкции.

Еще раз о декомпозиции
Ассоциативное приближение

КП – коэффициент приближение
КГ – коэффициент
горизонтальных деталей
КВ – коэффициент вертикальных
деталей
КД – коэффициент диагональных
деталей

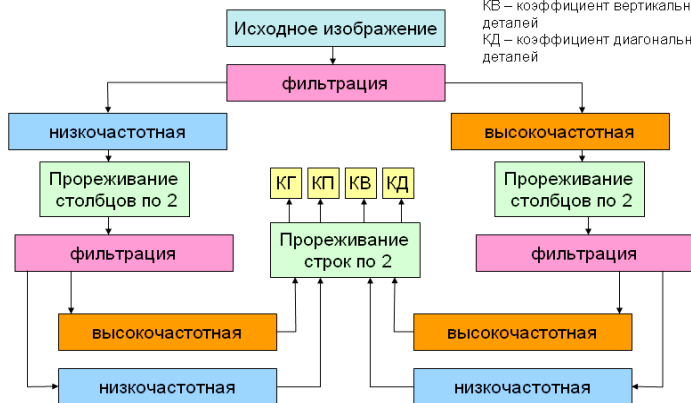


Рис. 1. Ассоциативное приближение декомпозиции

Подобно преобразованию Фурье, вейвлетные преобразования могут применяться при решении задач широкого спектра, от обнаружения контуров и до сглаживания изображений. В данном проекте используется фильтрация радиолокационного сигнала.

Радиолокационный сигнал представлен в виде монохромного изображения.

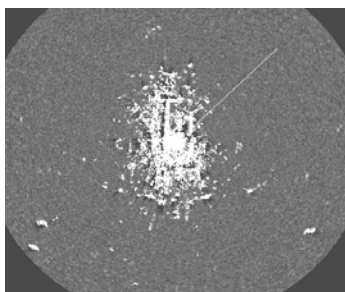


Рис. 2. Отображение сигнала на индикаторе РЛС

Для обработки данного сигнала используем программный пакет MATLAB.

На рис. 3. представлено считанное изображение с применением гистограммной эквализации, которая увеличивает динамический диапазон уровня яркости. На изображении отчетливо видны шумы.



Рис. 3. Считанное изображение (обработанное)

Обработка радиолокационного изображения будет произведена несколькими Вейвлет-функциями. В дальнейшем будет выбрана наилучшая из них.

Исследуемые Вейвлет функции: Хаара, Добеши, Симлета, биортогональная, Антонии–Добеши.

Преобразование Хаара является простейшим вейвлетным преобразованием, однако уже на этом простом примере обнаруживаются замечательные свойства этих преобразований. Оказывается, что поддиапазоны низкого уровня состоят из несущественных особенностей изображения, поэтому их можно смело квантовать и даже отбрасывать. Это дает хорошее сжатие с частичной потерей информации, которая, однако не отразится на качестве восстановленного образа. Реконструкция образа делается очень быстро с минимальной потерей качества [3].

Наилучшая фильтрация достигалась при фильтрации функцией Хаара. На рис. 4. представлен ее результат.



Рис. 4. Гистограммная эквализация изображения после фильтрации функцией Хаара

Вейвлет-фильтрация позволяет добиться наилучших результатов отображения, по сравнению с другими методами.

ЛИТЕРАТУРА

1. Гонсалес Р., Вудс Р., Эддинс С. Цифровая обработка изображений в среде MATLAB – М.: Техносфера, 2006. – 616 с.
2. Уэллетид С. Фракталы и вейвлеты для сжатия изображений в действии. – М.: Триумф, 2003. – 320 с.
3. Сэломон Д. Сжатие данных, изображений и звука. – М.: Техносфера, 2004. – 368 с.

**СИСТЕМА ПЕРЕДАЧИ ДАННЫХ ДЛЯ «РОЯ»
НАНОСПУТНИКОВ CUBESAT 3U
НА БАЗЕ СТАНДАРТА IEEE 802.16M**

Д.М. Орлов, студент

Научный руководитель А.М. Голиков, доцент каф. РТС, к.т.н.

г. Томск, ТУСУР, каф. РТС, rts2_golikov@mail.ru

Система передачи данных для «роя» наноспутников CubeSat 3U на базе стандарта IEEE 802.16m предназначена для передачи сигналов радиомаяка, приёма команд управления, передачу телеметрической информации и данных, полученных от полезной нагрузки.

Стандарт IEEE 802.16m использует три метода передачи данных: метод модуляции одной несущей (SC), метод ортогонального частотного мультиплексирования (OFDM) и метод множественного доступа на основе такого мультиплексирования (OFDMA). Спецификация физического уровня WirelessMAN-OFDM является наиболее интересной с точки зрения практической реализации. Она базируется на технологии OFDM, что значительно расширяет возможности оборудования, в частности, позволяет работать на относительно высоких частотах в условиях отсутствия прямой видимости. Кроме того, в нее включена поддержка топологии «каждый с каждым» (mesh), при которой абонентские устройства могут одновременно функционировать и как базовые станции, что сильно упрощает развертывание сети и помогает преодолеть проблемы прямой видимости.

Термином «CubeSat» обозначаются малые космические аппараты (МКА). Размер базового элемента конструкции спутника $10 \times 10 \times 10$ см. Стандарт допускает объединение двух и более стандартных кубов в составе одного спутника (обозначаются 2U, 3U и т.д.). Развитие современных высокотехнологичных отраслей позволило создавать малогабаритные космические аппараты при сравнительно небольших затратах времени и средств. При этом они способны решать серьезные научно-технические, исследовательские и промышленные задачи.

Организация беспроводной сети передачи данных между МКА позволяет обеспечить создание управляемой локальной группировки КА. Это дает возможность разместить на МКА, распределенную, перестраиваемую полезную нагрузку. Состав предлагаемой радиосети КА представлен на рис. 1 (ЦМКА – центральный МКА, ОМКА – оконечный МКА, НСУ – наземная станция управления).

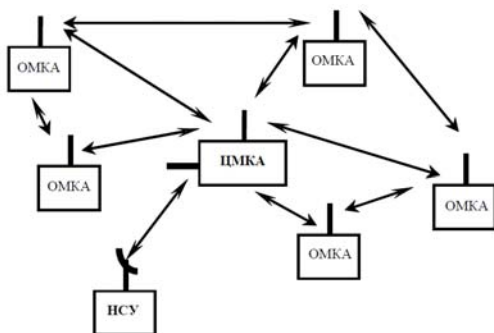


Рис. 1. Организация беспроводной сети передачи данных между МКА



Рис. 2. Внешний вид OMKA

Схема исследуемой системы:

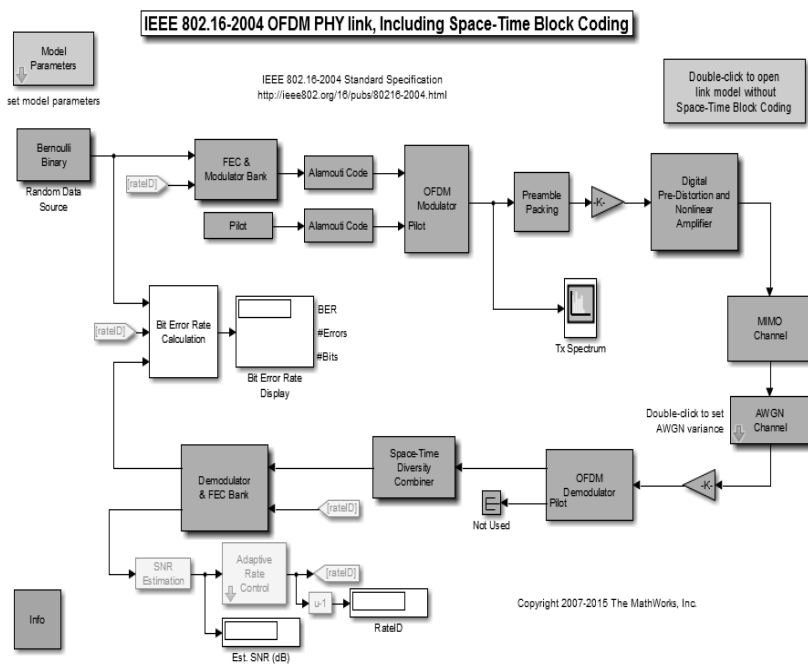


Рис. 3. Схема системы

Зависимости BER (битовой вероятности ошибки) от SNR (отношение сигнал / шум) для каждого конкретного вида модуляции приведены на рис. 4.

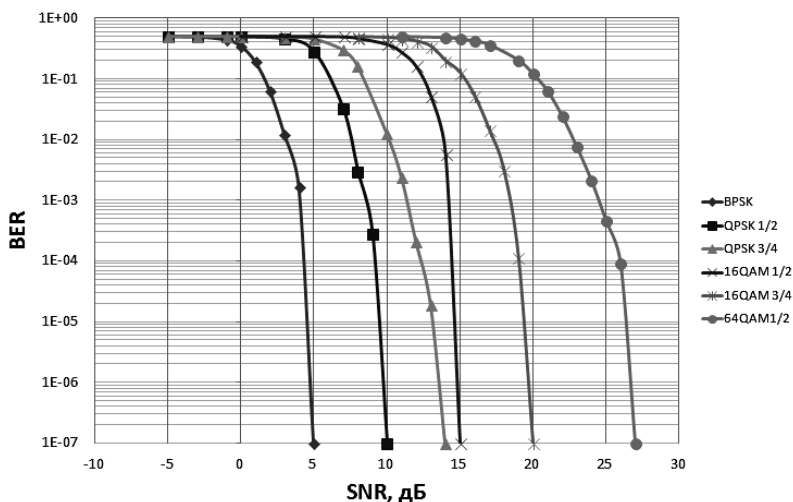


Рис. 4. Зависимости BER от SNR для отдельных видов модуляции

Энергетический расчет линии связи отвечает на наиболее часто встречающийся в тематике беспроводной связи вопрос: возможна ли связь на интересующем расстоянии и каково её качество.

Таблица 1

Данные для расчета

Рабочая частота	1500 МГц
Расстояние между точками	200 км
Мощность передатчика	37 дБм
Усиление антенны передатчика	21 дБi
Потери в кабеле 1 разъема	1 дБм
Потери в кабеле 2 разъема	1 дБм
Чувствительность приёмника	-85 дБм
Усиление антенны приемника	21 дБi

Таблица 2

Результаты расчета

Потери в свободном пространстве	141,9 дБ
Уровень сигнала на входе приемника	-64,9 дБм
Запас по энергетике канала	20,1 дБ

По результатам моделирования запас по энергетике канала составляет не менее 20 дБ, что позволяет утверждать о выполнении устойчивой связи.

ЛИТЕРАТУРА

1. Фатеев В.Ф., Каргу Д.Л. Практический опыт разработки элементов наноспутников серии «CubeSat» // Изв. вузов. Приборостроение. – 2006. – Т. 50. – С. 14–16.
2. Бараш Л.Е. Многообразие стандартов беспроводных технологий // Компьютерное обозрение. – 2003. – С. 25–28.

ЗАЩИЩЕННАЯ MESH-СЕТЬ ДЛЯ «РОЯ» БПЛА

М.С. Смолин, Ю.С. Хило, студенты

Научный руководитель А.М. Голиков, доцент каф. РТС, к.т.н.

г. Томск, ТУСУР, каф. РТС, rts2_golikov@mail.ru

Проект ГПО РТС-1603 «Разработка защищённых методов построения систем связи для беспилотных летательных аппаратов»

Наиболее эффективное управление «роем» БПЛА предоставляет Mesh-сеть. Информационные сети, организованные по топологии Mesh, получили в последнее время признание. Масштабы проектов выросли до тысяч точек доступа и десятков тысяч пользователей. Mesh-сети представляют наиболее интересные решения, интегрирующие различные сетевые и радиотехнологии, и потому в полной мере отвечают все более растущим требованиям абонентов (мобильность, QoS, безопасность).

Существующие в настоящее время Mesh-сети построены с использованием наиболее распространенного беспроводного стандарта IEEE 802.11s. Преимущества такого решения очевидны – широкий спектр дешевых стандартных абонентских устройств определяет коммерческую успешность проектов.

В настоящий момент не существует точных критериев, определяющих термин Mesh-сеть в применении к системам широкополосного беспроводного доступа. Наиболее общее определение звучит как: «Mesh – сетевая топология, в которой устройства объединяются многочисленными (часто избыточными) соединениями, вводимыми по стратегическим соображениям». В первую очередь понятие Mesh определяет принцип построения сети, отличительной особенностью которой является самоорганизующаяся архитектура, реализующая следующие возможности:

- создание зон сплошного информационного покрытия большой площади;
- масштабируемость сети (увеличение площади зоны покрытия и плотности информационного обеспечения) в режиме самоорганизации;

- использование беспроводных транспортных каналов (backhaul) для связи точек доступа в режиме «каждый с каждым»
- устойчивость сети к потере отдельных элементов [1].

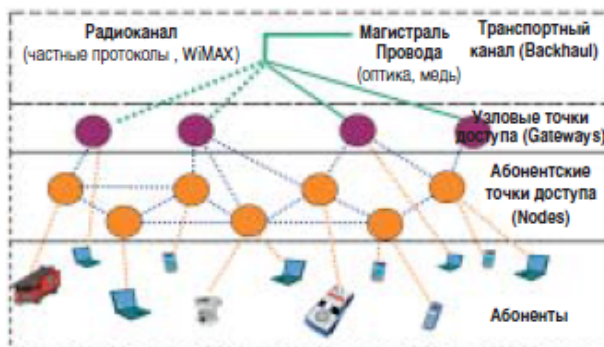


Рис. 1. Архитектура Mesh-сети

Топология Mesh основана на децентрализованной схеме организации сети, в отличие от типовых сетей IEEE 802.11s которые создаются по централизованному принципу. Точки доступа, работающие в Mesh-сетях, не только предоставляют услуги абонентского доступа, но и выполняют функции маршрутизаторов/ретрансляторов для других точек доступа той же сети. Благодаря этому появляется возможность создания самоустанавливающегося и самовосстанавливающегося сегмента широкополосной сети.

Принятие стандарта 802.11s (WPA2) делает доступной более безопасную схему аутентификации и кодирования трафика. Стандарт IEEE 802.11i предусматривает использование в продуктах Wi-Fi таких средств, как поддержка алгоритмов шифрования трафика: TKIP (Temporal Key Integrity Protocol), WRAP (Wireless Robust Authenticated Protocol) и CCMP (Counter with Cipher Block Chaining Message Authentication Code Protocol). Этих алгоритмов достаточно для защиты на уровне абонентского трафика, но на уровне корпоративного пользователя используются дополнительные механизмы, включающие более совершенные способы аутентификации при подключении к сети: более криптостойкие методы шифрования, динамическую замену ключей шифрования, использование персональных межсетевых экранов, мониторинг защищенности беспроводной сети.

Так же стандарт IEEE 802.11s предоставляет хорошую зависимость битовой вероятности ошибки BER от отношения сигнал/шум SNR.

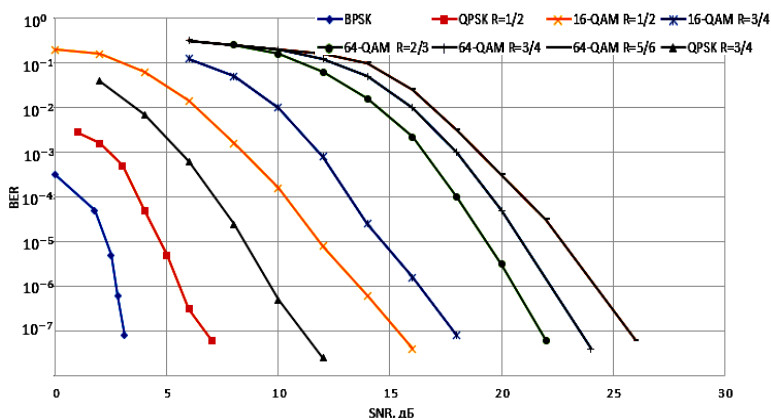


Рис. 2. График зависимости BER от SNR, для IEEE 802.11s

Внедрение новых спецификаций стандарта Wi-Fi (особенно IEEE 802.11s) обещает существенное увеличение скорости передачи информации, что в полной мере может компенсировать недостатки стандарта (коллизийность доступа, проявляющаяся в наибольшей степени в условиях высокой загрузки сети).

В работе рассмотрена возможность использования Mesh-сети для организации передачи данных «роя» БПЛА. Стандарт IEEE 802.11s обеспечивает широкополосную адаптивную передачу данных на расстояние до 8 км.

ЛИТЕРАТУРА

1 Simulink Model of the IEEE 802.11s PHY Layer model [Электронный ресурс]: Матер: сайта mathworks – разработчика ПО. – Режим доступа: <https://www.mathworks.com/matlabcentral/fileexchange/22137-simulink-model-of-the-ieee-802-11n-phy-layer-model>

АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС QNAP NS-256-PRO+ И WEB-САЙТ «СИСТЕМОТЕХНИКА РТС»

А.Р. Усманова, студентка

*Научный руководитель А.М. Голиков, доцент каф. РТС, к.т.н., с.н.с.
г. Томск, ТУСУР, каф. РТС, rts2_golikov@mail.ru*

*Проект ГПО РТС-1507 «Разработка Web-сайта научно-технической
«Системотехники РТС» на основе аппаратно-программного
комплекса QNAP TS-259 PRO+»*

Аппаратно-программный комплекс QNAP NS-256-PRO+ представляет собой специализированный сервер. Включает двухъядерный и четырехпоточный D510 процессор. Частота – 1,66 ГГц.

Остальные характеристики включают в себя – два гигабитных сетевых контроллера 82574L, модуль памяти SODIMM 1 Гб DDR2-800, флеш-диск объемом 512 Мб и интерфейсом USB.

В рассматриваемом двухдисковом устройстве нет необходимости использовать какие-либо внешние контроллеры, кроме сетевых, поскольку все остальное (SATA и USB) – уже встроено в чипсет.



Рис. 1. Внешний вид QNAPTS-256-PRO+

Модель имеет графический контроллер и порт VGA, что позволяет использовать ее как полнофункциональные мини-ПК.

Преимущества аппаратно-программного комплекса QNAPTS-256-PRO+:

1. Управление дисковым пространством:

- Изменение уровня RAID без остановки работы накопителя (с помощью этой функции можно, купив диски, создать RAID-массив без потери данных и отключения хранилища от сети).

- Средства диагностики жестких дисков (технология S.M.A.R.T. позволяет отслеживать состояние жесткого диска с помощью встроенной аппаратуры самодиагностики, накопитель может производить проверку жестких дисков и сканирование на наличие ошибок по технологии HHS).

- Сетевое хранилище и iSCSI (хранилище может использоваться одновременно для предоставления общего доступа к ресурсам и в качестве клиента/сервера iSCSI. Благодаря встроенной функции «Виртуальный диск» (VirtualDiskDrive) можно легко увеличить емкость дискового пространства хранилища.

2. Кластеры и платформы виртуализации:

Сетевые хранилища QNAP Turbo NAS для бизнеса получили сертификат VMware как подтверждение их совместимости с облачной платформой виртуализации vSphere. Благодаря реализации таких функций, как MC/S (множество соединений на сессию), MPIO (многопутевый ввод-вывод) и Thin-provisioning (экономное распределение дискового пространства), сервер QNAP представляет собой готовое решение хранения для отказоустойчивых кластеров или платформ виртуализации. Turbo NAS может выступать в роли хранилища дан-

ных как для VMware, так и для кластеров и платформ виртуализации в среде Microsoft.

3. Преимущество двух интерфейсов GigabitEthernet:

- Отказоустойчивость.
- Балансировка нагрузки.
- Режим Multi-IP.

4. Готовое решение резервирования данных:

- Утилита NetBakReplicator.
- Поддержка ПО сторонних производителей.
- Репликация ресурсов накопителя по протоколу RSync.
- Управление резервным копированием AppleTimeMachine.
- Облачное резервирование данных.
- Репликация в реальном.
- Копирование с фотокамеры/USB-диска.

5. Возможности сервера:

- Кроссплатформный файловый сервер.
- FTP-сервер.
- Менеджер загрузки.
- Веб-сервер и сервер MySQL.
- Медиапортал.
- UPnP-медиасервер.
- Сервер iTunes.
- Принт-сервер.
- Работа с ISO-образами.
- Управление пользователями и ресурсами.
- Приложение QMobile для мобильных устройств Apple и Android.

- Поддержка ActiveDirectory.
- Платформа QPKG.

6. Управление и системные инструменты:

- Блокирование IP-адресов на базе.
- Планировщик работы устройства.
- Служба SNMP.
- Спящий режим.
- Автоматическое управление системным вентилятором.
- Оповещения по E-mail и SMS.
- Защищенное подключение по протоколам SSH и SSL (HTTPS).
- Системный журнал.
- Подробная информация о системе.

7. Система видеонаблюдения:

- Сервер видеонаблюдения с поддержкой IP-камер ведущих производителей.

- Аудио- и видеомониторинг, запись и воспроизведение через Интернет.

8. Управление питанием:

- Режим ожидания для жестких дисков.
- Планировщик работы устройства.
- Функция Wakeon LAN.

В результате выполнения данной работы была произведена установка программного обеспечения и испытание режимов работы сервера, а также разработан сайт «Системотехника РТС». Сайт заполнен контентом и готов к работе.

ЛИТЕРАТУРА

1. Хакен Граф. Руководство для начинающего пользователя Joomla 2.5: Пер. с англ. А. Баскинов. – М.: Гелиос, 2012 – 243 с.
2. Кочетков К. Два по два. – Ч. 2:– сетевые накопители QNAP TS-239 Pro II и TS-259 Pro [Электронный документ]. – URL: <http://www.ixbt.com/storage/storage-qnap-ts-2x9-2.shtml>

МОДЕЛИРОВАНИЕ И ИССЛЕДОВАНИЕ ГЕНЕРАТОРА ПСЕВДОСЛУЧАЙНЫХ СИГНАЛОВ НА ОСНОВЕ НЕЛИНЕЙНЫХ ДИНАМИЧЕСКИХ СИСТЕМ ЧУА

Д.А. Ишмуков, студент

Научный. руководитель В.В. Афанасьев, проф., д.т.н.

*г. Казань, КНИТУ им. А.Н. Туполева-КАИ, Ishmukov@gmail.ru,
ivans8585@mail.ru*

Оптимизация систем конфиденциальной цифровой передачи информации, использующей эффекты динамического хаоса, неразрывно связана с разработкой и исследованием моделей формирователей многомерных хаотических сигналов на основе дискретно-нелинейных систем [1, 2]. В докладе рассматривается разработка и исследование генератора псевдослучайных сигналов на основе дискретно-нелинейной динамической системы Чуа [3, 4]. В качестве платформы для проведения моделирования, выбрана интерактивная среда для программирования – MathLAB.

Цель работы – исследование зависимости работы генератора псевдослучайных сигналов от изменения параметров системы Чуа. Смоделирована система Чуа, оценены статистические характеристики сигналов генератора псевдослучайных сигналов на базе дискретно-нелинейной системы Чуа при изменении параметров системы. Построены зависимости амплитуды колебаний генерируемых псевдо-

случайных сигналов от времени, построены фазовые портреты, сделаны выводы о реакции дискретно-нелинейной системы Чуа на изменения параметров и вариации начальных условий. Характерный фазовый портрет, полученные в результате моделирования системы Чуа, с параметрами $m_0 = -8/7$; $m_1 = -5/7$; $\alpha = 9.8$; $\beta = 110/7$; $c_1 = (m_0 - m_1)/2$ представлен на рис. 1.

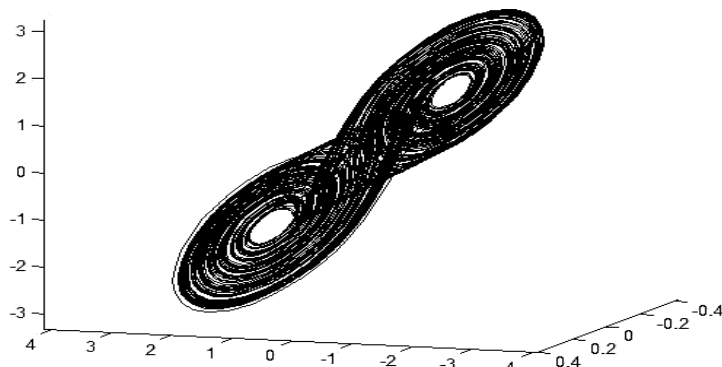


Рис. 1 Фазовый портрет системы Чуа

В таблице представлены значения дисперсии, математического ожидания и среднеквадратического отклонения сигналов X , Y , Z моделируемой дискретно-нелинейной системы Чуа при различных параметрах системы.

Статистические характеристики генерируемых сигналов

Сигнал	Параметры системы Чуа	
	$m_0 = -8/7, m_1 = -5/7$	$m_0 = -9/7, m_1 = -6/7$
X	$\text{disp}(X) = 1,9505$ $M(X) = 0,0147$ $\text{CKO}(X) = 1,3966$	$\text{disp}(X) = 8,6852$ $M(X) = 0,0701$ $\text{CKO}(X) = 2,9471$
Y	$\text{disp}(Y) = 0,0317$ $M(Y) = 2,637^{(-4)}$ $\text{CKO}(Y) = 0,1779$	$\text{disp}(Y) = 0,1616$ $M(Y) = 9,197^{(-4)}$ $\text{CKO}(Y) = 0,4023$
Z	$\text{disp}(Z) = 2,5067$ $M(Z) = -0,0110$ $\text{CKO}(Z) = 1,5833$	$\text{disp}(Z) = 11,6334$ $M(Z) = -0,0551$ $\text{CKO}(Z) = 3,4108$

По результатам проведенных исследований вырабатываются инженерные рекомендации по выбору параметров генераторов псевдо-случайных сигналов на основе системы Чуа.

Таким образом, разработанные средства моделирования могут быть применены для исследования и оптимизации параметров систем конфиденциальной цифровой передачи информации, использующей эффекты динамического хаоса на базе генераторов сигналов дискретно-нелинейной системы Чуа.

ЛИТЕРАТУРА

1. Кузнецов С.П. Динамический хаос: учеб. пособие для вузов. – 2-е изд. перераб. и доп. – М.: Изд-во физ.-мат. лит-ры, 2006. – 356 с.
2. Афанасьев В.В., Логинов С.С., Польский Ю.Е. Анализ и синтез нелинейных радиоэлектронных динамических систем и устройств с варьируемым шагом временной сетки. – Казань: Изд-во Казан. гос. техн. ун-та, 2013. – 231 с.
3. Афанасьев В.В., Логинов С.С. Импульсные случайные процессы в анализе и диагностике нелинейных систем с динамическим хаосом // Радиотехника и электроника. – 2013. – Т. 58, № 4. – С. 382–388.
4. Афанасьев В.В., Логинов С.С., Польский Ю.Е. Формирователи двоичных псевдослучайных сигналов на основе управляемых систем Лоренца и Чуа // Телекоммуникации. – 2012. – № 12. – С. 26–30.

ПОДСЕКЦИЯ 4.3

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

*Председатель секции – Кузьмина Е.А., доцент каф. КИБЭВС, к.т.н;
зам. председателя – Глухарева С.В., ст. преп. каф. КИБЭВС*

БЛАГОНАДЕЖНЫЙ СОТРУДНИК В СИСТЕМЕ КАДРОВОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

М.Е. Абросимова, студентка

С.В. Глухарева, ст. преп. каф. КИБЭВС

г. Томск, ТУСУР, каф. КИБЭВС, abrosimovaamaria@outlook.com

*Проект ГПО КИБЭВС01517 «Система кадровой
безопасности предприятия»*

В настоящее время рынок все больше развивается и расширяется, возрастает конкуренция на рынке, в следствие чего все большее внимание уделяется подбору благонадежных сотрудников, от которых в первую очередь зависит деятельность любой организации. Условия жестокой конкуренции, введения профессиональных стандартов, развитие информационных технологий, повышенное внимание к безопасности компании и её будущему – все это говорит о повышении требований к сотруднику. Сейчас сотрудник должен обладать не только личными и профессиональными компетенциями, но и должен отвечать требованиям безопасности, быть ориентированным на будущее, отвечать требованиям работодателя и разделять ценности компании. Все это способно определить благонадежного сотрудника.

В настоящее время нет его единого определения «благонадежного сотрудника». Обратимся к этимологии слова «благонадежный»: в «Толковом словаре русского языка» С.И. Ожегова и Н.Ю. Шведовой благонадежный означает «заслуживающий доверия» [2]. В «Толковом словаре живого великорусского языка» В.И. Даля дано более обширное определение, которое определяет его как «...твердый в надежде, не сомневающийся; надежный, несомненный, верный, на кого можно надеяться, положиться» [3]. Под благонадежностью, как качеством личности, современники понимают «склонность связанную с принципами человека соблюдать принятые в обществе правила, ценности и

нормы поведения» [4]. Таким образом, опираясь на приведенную выше терминологию сделаем вывод, что под благонадежным сотрудником будем понимать надежного сотрудника, отвечающего профессиональным требованиям работодателя, разделяющего ценности компании и общества, а также готового работать на развитие себя и компании в целом.

В рамках системы кадровой безопасности предприятия уровень благонадежности сотрудника определяется, исходя из личных профессиональных, специальных компетенций, а также корпоративных компетенций, компетенций будущего, и компетенций безопасности.

На сегодняшний день существует множество классификаций компетенций, каждая из которых, «определяется социумом, имеет различия в разных странах мира и зависит от ценностных ориентаций, правил существования, мировоззрения отдельного сообщества» [5]. Но большинство компаний при трудоустройстве работника используют в основном только личные и профессиональные компетенции. Они не учитывают особенности своей деятельности, условия развивающейся действительности, ожесточенной конкуренции и повышение требований к компетенциям персонала. Необходимо определять безопасность сотрудника, его ориентированность на будущее, способность подстраиваться под условия изменяющихся условий и требований, только учитывая и анализируя все эти факторы возможно определить уровень благонадежности сотрудника.

Для определения уровня благонадежности разработана модель компетенций, которая учитывает специфику отрасли, в которой действует организация, особенности компании, функционал должности (основной и дополнительный), изменяющиеся условия, вопросы безопасности. В модели компетенции определяются такие группы компетенций как: личные, профессиональные, корпоративные, безопасности, будущего, специальные, специально-психологические, поведенческие и компетенции успешности.

Среди корпоративных компетенций большое значение имеют такие компетенции, как лояльность, социальный интеллект, клиентоориентированность, социальная гибкость и проницательность. Каждая из названных компетенций напрямую влияет на кадровую безопасность предприятия. Сотрудник, не разделяющий ценностей компании, не заинтересованный в успешной деятельности компании, не способный брать на себя ответственность, не ориентированный на результат – не способен отвечать требованиям организации. Данный сотрудник не несет никакой ценности, а лишь наоборот, только подвергнет риску её безопасность и успешность.

Умение просчитывать риски, самообладание, самоконтроль и другие занимают важное место среди компетенций безопасности. Особое внимание стоит обратить на оценку уровня эмоционального интеллект сотрудника (EQ), ведь на сегодняшний день оценка уровня интеллекта (IQ) отходит на второй план. Важность EQ объясняется тем, что он, по сравнению с IQ, способен объяснить особенности поведения и мотивации людей. Сотрудник, владеющей данной компетенцией, способен управлять своими эмоциями, подстраиваться под окружающую среду, улавливать чужое настроение и действовать в зависимости от этого, за счет чего повышается уровень безопасности предприятия.

Быстро изменяющиеся условия рынка и труда, появление новых информационных технологий, внедрение «искусственного разума» приводит к тому, что требования работодателя к сотруднику меняются. Сегодня сотруднику необходимо выполнять один набор функций, через 2–3 года, этот набор очень резко видоизменяется. Следовательно, особое место необходимо уделять таким компетенциям как гибкость к изменениям, проницательность, фасеточное мышление, когнитивная гибкость и умение предвидеть. Владение этими компетенциями обеспечит его востребованность в будущем.

В основе определения уровня благонадежности лежит теория нечетких множеств и определяется как коэффициент от 0 до 1, подразделяясь на «высокий», «средний» и «низкий» уровень благонадежности. Коэффициент «высокого» уровня находится в диапазоне от 0,6 до 1, «средний» от 0,3 до 0,6, и «низкий» соответственно от 0 до 0,3. Но нельзя забывать о том, что совершенных людей не существует, следовательно, и не может быть сотрудника с коэффициентом равным 1, поэтому мы будем рассматривать сотрудника с уровнем благонадежности выше 0,51, для дальнейшей работы с ними.

Подводя итог всему вышесказанному, можно сделать вывод, что компетенции являются основополагающим для определения уровня благонадежности сотрудника. А благонадежный сотрудник в свою очередь составляет основу для кадровой безопасности. Такой сотрудник ориентирован на будущее, лоялен, с высоким уровнем эмоционального интеллекта и владеющий другими компетенциями, необходимыми при условиях жесткой конкуренции в условиях развивающегося рынка и условиях повышенного внимания к безопасности предприятия.

ЛИТЕРАТУРА

1. Крылов А. Цифровую революцию в HR можно не ждать – она уже началась // Harvard Business Review [Электронный ресурс]. – URL: <http://hbr-russia.ru/innovatsii/startap/a21891/> (дата обращения 10.03.2017).

2. Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений // Российская академия наук. Институт русского языка им. В.В. Виноградова. – 4-е изд., доп. – М.: Азбуковник, 1999. – 944 с.

3. Даль В.И. Толковый словарь живого великорусского языка / Товарищество М.О. Вольф. – СПб., М., 1903. – Т. I.

4. Федорова А.Э., Некрасова Л.В. Исследование кадровых рисков и факторов благонадежности персонала промышленного предприятия // Вестн. Ом. ун-та. Сер. «Экономика». – 2017. – №4 (60). – С. 123–135.

5. Калужная Н.В. Разработка модели компетенций организации // Молодой ученый. – 2016. – №6. – С. 447–455 [Электронный ресурс]. – URL: <https://moluch.ru/archive/110/27084/> (дата обращения: 12.03.2018).

МЕТОДЫ МИНИМИЗАЦИИ РИСКОВ КРЕДИТОВАНИЯ ФИЗИЧЕСКИХ ЛИЦ

А.А. Червинская, студент

*Научный руководитель Е.И. Губин, доцент каф. КИБЭВС, к.т.н.
г. Томск, ТУСУР, каф. КИБЭВС, alyona_chervinskaya@mail.ru*

Нормальное функционирование банковской системы является необходимым условием экономической безопасности страны. Обеспечение финансовой устойчивости банковской деятельности – это одна из основных задач, которую необходимо решать любому банку. Неграмотно выстроенная кредитная политика и неадекватная оценка кредитных рисков приводят к серьезным проблемам и в том числе банкротству финансово-кредитных учреждений.

В период нарастающей конкуренции между банками, каждый стремится увеличивать свой кредитный портфель. Они привлекают потенциальных заемщиков за счет упрощения условий кредитования (отсутствие поручителей, залога, уменьшение пакета необходимых документов) – это увеличивает кредитные риски банка. Процедура оценки кредитоспособности заемщика, занимающая большое количество времени с предоставлением объемного пакета документов, значительно снижает риск невозврата кредита, но может оттолкнуть кредитоспособных заемщиков от услуг такого банка. В таких условиях нужно постоянно разрабатывать методы снижения кредитных рисков и в то же время склонить потенциального заемщика к использованию услуг такого банка.

Кредитование считается более распространенным инструментом размещения банковских ресурсов. В целом за период с 2011–2018 гг. объем кредитов, выданных населению, увеличился более чем в 2 раза [1].

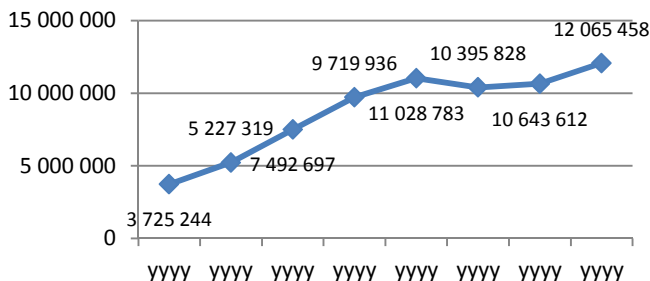


Рис. 1. Объем кредитов, предоставленных физическим лицам в 2011–2018 гг. в млн. руб.

Из рис. 1 видно, что объемы кредитов растут на протяжении с 2011 по 2018 гг., но произошел резкий спад объема выданных кредитов с 2015 по 2016 г. Первая причина тому – сложная ситуация в экономике и выросшая закредитованность населения. Банки существенно скорректировали свои модели управления рисками и требования к заемщикам стали жестче, а согласованные суммы кредитов меньше. Вторая причина – для минимизации инфляционных рисков ЦБ РФ повысил ключевую ставку, в этот период она увеличивалась до максимальных значений – с 10,5% до 17%, что вызвало увеличение процентных ставок коммерческих банков.

За период с 2011–2018 гг. объем задолженности по кредитам, выданных населению, увеличился более чем в 1,5 раза.

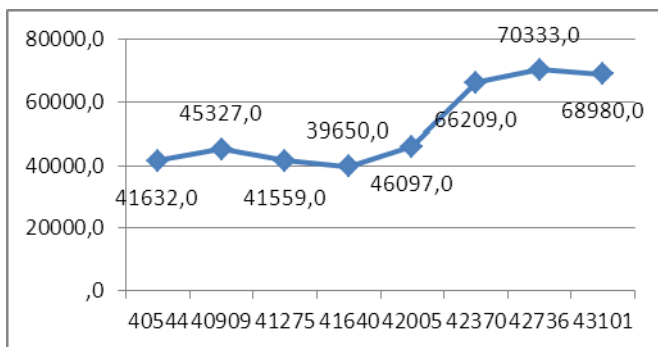


Рис. 2. Объем просроченной задолженности по кредитам, предоставленным кредитными организациями физическим лицам в 2011–2018 гг. в млн. руб.

Из рис. 2 видно, что объем просроченной задолженности по кредитам имеет высокий рост с 2015 по 2018 гг. Темпы роста объема просроченной задолженности по кредитам с 2015 по 2018 гг. значительно больше, чем темпы роста выдачи кредитов, предоставленных физическим лицам. Следовательно, некоторым кредитным организациям стоит пересмотреть политику в отношении выдачи кредитов физическим лицам, тем самым минимизировать риски неуплаты.

Оценка экспертов показывает, что доля просроченной задолженности по кредитованию населения в портфелях российских банков в 2016 г. снизилась с 8,1% на 1 января 2016 г. до 7,9% на начало 2017 г. [2]. В международной практике кредитования оптимальным уровнем просроченных кредитов считается 4–5%. Так как данный коэффициент выходит за рамки, то проблемы эффективного управления рисками кредитования физических лиц занимают центральные места в данное время.

Минимизировать риски возможно как на этапе рассмотрения документов потенциального заемщика, так и в процессе кредитования (в период действия кредитного договора). Методы минимизации рисков указаны на рис. 3 [3].



Рис. 3. Методы минимизации рисков кредитования физических лиц

Данные методы взаимосвязаны между собой и часто являются производными друг от друга и дополнениями друг друга, следовательно, чтобы получить эффективный результат, нужно применять их в комплексе.

ЛИТЕРАТУРА

1. Статистические данные Банка России [Электронный ресурс]. – Режим доступа: <http://www.cbr.ru/statistics/> (дата обращения: 25.02.2018).

2. Рейтинг регионов по доле задолженности просроченной населением [Электронный ресурс]. – Режим доступа: <http://riarating.ru/regions/20170323/630059013.html> (дата обращения: 01.11.2017).

3. Погребняк Е.Н. Риски кредитования населения и современные методы управления ими 2013 г. [Электронный ресурс]. – Режим доступа: <https://research-journal.org/economical/riski-kreditovaniya-naseleniya-i-sovremennyye-metody-upravleniya-imi/> (дата обращения: 29.10.2017).

АНАЛИЗ СОВРЕМЕННЫХ СРЕДСТВ ПОЛУЧЕНИЯ КРИПТОВАЛЮТ

А.В. Куртукова, П.А. Дятлова, студенты;

А.С. Романов, доцент каф. БИС, к.т.н.

*г. Томск, ТУСУР, av.kurtukova@gmail.com, dyatlova.98@inbox.ru,
alex.romanov@gmail.com*

За стремительным развитием мировой экономики неизбежно следует и внедрение новых технологий. Одной из таковых стала криптовалюта, как разновидность цифровой валюты, основанная на криптографических методах и технологии блокчейна. Существует мнение, что криптовалюты способны стать эффективным решением проблем безопасности денежного оборота.

Рассмотрим потенциальные риски использования криптовалют, связанные со спецификой и принципами их работы:

1. Отсутствие всяких гарантий. Пользователь криптовалют никак не может быть застрахован от потери ключа доступа или криптографической подписи, позволяющих производить операции с криптовалютой, т.е. пользователь персонально несет ответственность за имеющиеся сбережения.

2. Высокая волатильность. Подавляющее большинство потенциальных инвесторов предпочитают отгородить себя от рисков, связанных с нестабильностью курса виртуальных валют, и делают выбор в пользу фидуциарной валюты.

3. Неустойчивая позиция государства. В настоящее время криптовалюты представляют собой независимые от государств всего мира системы обмена виртуальными денежными средствами. Для последних такая ситуация может привести к угрозам национальным валютам, заключающимся в отсутствии контроля денежных потоков, возникновении благоприятных условий для оборота нелегальных товаров, анонимности сторон, заключающих сделки.

4. Мошенничество в области цифровой валюты. Наиболее распространенные виды мошенничества: финансовые пирамиды и фи-

шинговые сайты, зачастую несущие в себе не только опасность кражи персональных данных, но и получения вредоносного ПО.

Несмотря на ряд значительных недостатков, популярность криптовалют вполне обусловлена следующими факторами:

1. Децентрализация. Данной особенностью обуславливается отсутствие центра эмиссии. Все распределенные по миру дата-центры, обеспечивающие обработку данных, поддерживают саму деятельность платформы и получают за это вознаграждение в виде комиссионных сборов в определенной криптовалюте. Такой процесс называется майнингом, а пользователи, расходующие имеющиеся у них вычислительные мощности – майнерами.

2. Безусловная прозрачность операций. Все данные по транзакциям остаются в единой базе данных навсегда, что позволяет в любой момент времени проверить необходимую информацию и отследить историю действий.

3. Анонимность. Использование виртуальных валют осуществляется без предъявления удостоверения личности. Неизбежное следствие – отсутствие всякой информации, помимо номера счета и его состояния, о владельце криптовалютного кошелька.

4. Как правило, выпуск криптовалют является ограниченным, за счет чего становится возможным избежание обесценивания виртуальных денег. Эта особенность является особенно важной в связи с проблемой инфляции и позволяет вовлекать инвесторов, стремящихся сохранить свои сбережения.

В связи с активным распространением криптовалюты и её поступательным поглощением фидуциарной валюты возникает необходимость в детальном рассмотрении основных способов майнинга. Наиболее распространенными являются:

1. GPU-фермы, работающие за счёт мощности графических процессоров;

2. FPGA-модули, перенастраиваемые конечным пользователем;

3. ASIC-майнеры, действующие на базе процессоров.

Критически важным в процессе добычи криптовалют критерием является хешрейт (число циклов подбора хешей, выполняемое оборудованием в секунду), определяющий вычислительную мощность оборудования. Показатель энергопотребления оказывает прямое влияние на срок окупаемости. Рабочая температура обуславливает необходимые для содержания оборудования условия.

Несмотря на недостатки вышерассмотренных систем, каждая из них является благоприятной для конкретного вида криптовалют. В целом, тип оборудования, наиболее подходящего для майнинга, опре-

деляется алгоритмом, соответствующим конкретным криптовалютам. Например, Ethereum эффективнее добывается на GPU-фермах и модулях FPGA, чаще всего специализирующихся на алгоритмах Ethash и CryptoNight, Bitcoin на ASIC-майнерах, обычно применяемых к SHA-256. Исходя из этого, становится возможным расчет рентабельности оборудования для майнинга при добыче наиболее выгодной для него криптовалюты (табл. 2).

Таблица 1

Сравнительный анализ оборудования для майнинга криптовалюты

	Pulse Radeon RX580	Spartan-6 LX150T	AntMiner S9
Хешрейт (GH/s)	0,03	0,1	13500
Мощность (W)	225	12	1450
Стоимость (USD)	~ 450	~ 995	~ 2100
Температура (°F)	158	185	122
Энергопотребление (кВт·ч)	0,225	0,02	1,45
Эксплуатация (USD/мес.)	9,72	0,865	62,64

Таблица 2

Расчет рентабельности оборудования для майнинга

	Sapphire Pulse Radeon RX580 (ETH)	Spartan-6 LX150T (ETH)	AntMiner S9 (BTC)
1 день	0,002365	0,0069	0,001181
1 неделя	0,01655	0,0483	0,00826
1 месяц	0,0662	0,1932	0,0331
1 год	0,7946	2,3184	0,3968

Исходя из информации, представленной табл. 1 и 2, производится расчет окупаемости оборудования для майнинга с учетом затрат на электроэнергию.

Данные, приведенные в табл. 1 и 2, являются актуальными на февраль 2018 г. Величины энергопотребления соответствуют среднему тарифу по Томской области – 3,25 руб./кВт·ч (0,06 USD/ кВт·ч). Стоимость криптовалют: 1 BTC $\equiv$ 8080 UDS; 1 ETC $\equiv$ 812,5 UDS.

Таким образом, срок окупаемости ASIC-майнера AntMiner S9 составит 8 месяцев, видеокарты Sapphire Pulse Radeon RX580 – 9 месяцев и Spartan-6 LX150T – 7 месяцев (без учета амортизации).

ЛИТЕРАТУРА

1. Свон М. Блокчейн: Схема новой экономики / пер. с англ. – М.: Олимп-Бизнес, 2016. – 224 с.
2. Винья П., Кейси К. Эпоха криптовалют. Как биткоин и блокчейн меняют мировой экономический порядок – М.: Манн, Иванов и Фербер, 2017. – 432 с.

3. Mining hardware comparison [Электронный ресурс]. – Режим доступа: https://en.bitcoin.it/wiki/Mining_hardware_comparison, свободный (дата обращения: 2.02.18).

4. Статистика криптовалют [Электронный ресурс]. – Режим доступа: <https://bitinfocharts.com/ru/>, свободный (дата обращения: 9.02.18).

ВНЕДРЕНИЕ ИНФОРМАЦИОННО – АНАЛИТИЧЕСКОЙ СИСТЕМЫ «СПАРК» В УЧЕБНЫЙ ПРОЦЕСС ФАКУЛЬТЕТА БЕЗОПАСНОСТИ

А.Г. Вахитов, М.М. Джаналиев, Ю.А. Рубцова, студенты;

А.С. Колтайс, аспирант

Научный руководитель Е.М. Давыдова, доцент каф. КИБЭВС, к.т.н.

г. Томск, ТУСУР, каф. БИС и КИБЭВС, tusur1love@gmail.com

Проект ГПО КИБЭВС-1703 «Методика работы с системой СПАРК»

С развитием высоких технологий, актуальность использования электронных методов обучения в системе образования РФ высока. Во многих государствах, в том числе и в РФ, правительство поддерживает инициативу внедрения электронных методов обучения.

Большой шаг в становлении онлайн-образования в нашей стране является разработка проекта «Современная цифровая образовательная среда в Российской Федерации», утвержденного 25.10.2016 г. на заседании президиума Совета при Президенте Российской Федерации по стратегическому развитию и приоритетным проектам [1]. Электронное обучение в учебной деятельности ТУСУР в настоящее время набирает большую популярность, так как в 2016 г. учёным советом ТУСУР была принята концепция электронного обучения на 2016–2018 гг. [2].

Для увеличения эффективности обучения студентов, и овладения ими широкого спектра различных специальных и профессиональных компетенций, необходимо предоставлять доступ к различным специализированным информационно-аналитическим системам (ИАС) либо современным программным комплексам. К примеру, для решения задач, по осуществлению экономической и информационной безопасности на предприятии, существуют специализированные информационно-аналитические системы, позволяющие проверить надёжность любой организации, найти компании – потенциальных клиентов, удовлетворяющих определённым критериями, отслеживать изменения деятельности своих партнёров, разрабатывать политику безопасности предприятия. Для того чтобы будущие специалисты в области безопасности владели необходимыми навыками и были востребованы на

рынке труда, осуществилось внедрение специализированной информационно – аналитической системы «СПАРК» в учебные процессы ТУСУР, а именно на факультете безопасности. [3]

«Сетевое издание «Информационный ресурс СПАРК» – профессиональное решение для проверки контрагентов, управления кредитными и налоговыми рисками, маркетинга, инвестиционного анализа, поиска аффилированности. Основными достоинствами ИАС СПАРК являются:

- данные находятся в едином хранилище;
- данные предоставлены в удобном формате;
- доступ к различным аналитическим инструментам [4].

Для изучения ИАС СПАРК ранее был создан электронный курс в СУО Moodle состоящий из 9 тем, каждая из которых включает в себя:

- видеоурок;
- практическое задание;
- контрольный тест.

Прохождение данного учебного курса позволяет овладеть навыками работы с ИАС СПАРК, а также применять данную систему для изучения различных дисциплин, таких как, «Оценка рисков», «Финансовый анализ», «Анализ типологий финансовых махинаций», на протяжении всего процесса обучения.

ИАС СПАРК в рамках изучения дисциплин, позволяет решать определенные задачи, решение которых позволит студентам овладеть навыками и компетенциями в рамках своей специальности. Например, при внедрении такого курса, в учебные процессы студентов по направлениям «Экономическая безопасность (38.05.01)» и «Информационно – аналитические системы безопасности (10.05.04)», были разработаны, различного рода практические и лабораторные работы, для дисциплин «Математические методы в задачах финансового мониторинга», «Экономический анализ», «Основы финансового расследования», которые позволят студентам получить такие компетенции, как:

- способность проводить комплексный анализ функционирования финансовых и экономических структур государственного или системообразующего уровня с целью выявления угроз (отрицательных тенденций) национальной безопасности Российской Федерации;
- способность решать задачи выявления, классификации и последующего предметного анализа информационных объектов с признаками подготовки и/или совершения преступлений в финансовой и экономической сферах деятельности;
- всестороннее и детальное изучение на основе всех имеющихся источников информации различных аспектов функционирования дан-

ной организации, направленное на улучшение её работы путем разработки и внедрения оптимальных управленческих решений, отражающих резервы, выявленные в процессе проведения анализа и пути использования этих резервов.

Таким образом, в рамках проекта ГПО КИБЭВС–1703 «Методика работы с системой СПАРК» были разработаны задания с использованием ИАС СПАРК, для внедрения в учебные дисциплины, такие как: «Основы финансового расследования», «Методология и обеспечение информационно-аналитической деятельности», «Экономический анализ».

ЛИТЕРАТУРА

1. Приоритетный проект «Современная цифровая образовательная среда в РФ» [Электронный ресурс]. – Режим доступа: <http://www.минобрнауки.рф/проекты/современная-цифровая-образовательная-среда> (дата обращения: 18.02.2018).

2. Пекарских С.А., Колтайс А.С. Разработка и внедрение электронного курса по работе с информационным ресурсом «Спарк» в системе управления обучением (СУО) «Moodle» на факультете безопасности ТУСУР // Матер. четвертой Междунар. науч. конф. «Информационные технологии в науке, управлении, социальной сфере и медицине». – 2017. – С. 305–308.

3. Колтайс А.С., Конев А.А. Информационно-аналитическая система «СПАРК» при обеспечении экономической безопасности предприятия // Матер. первой Всерос. науч.-практ. онлайн-конф. «Экономическая безопасность: финансовые, правовые и IT-аспекты». – 2017. – С. 178–182.

4. О системе СПАРК [Электронный ресурс] – Режим доступа: <https://www.spark-interfax.ru/promo/ru/about> (дата обращения: 20.02.2018).

РЕКОМЕНДАТЕЛЬНАЯ СИСТЕМА КАДРОВОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

В.Е. Мальцев, А.С. Еременко, А.О. Селезнев, студенты;

С.В. Глухарева, ст. преп.

г.Томск, ТУСУР, каф. КИБЭВС, gsv@keva.tusur.ru

В наши дни очень важную роль в организации любого предприятия играет кадровая безопасность. Кадровая безопасность – это система предприятия, связанная с функционированием организации (предприятия) в условиях безопасности и с эффективной работой персонала, направленной на развитие самой организации в целом, и каждого сотрудника в отдельности. Задача кадровой безопасности заклю-

чается в проведении мероприятий, направленных на недопущение лиц к занятию должностных позиций, злоупотребляя которыми, они могут нанести своими действиями вред компании в соответствии с вышеперечисленными угрозами, а также в проведении постоянного мониторинга, направленного на обеспечение кадровой безопасности.

Создание конкурентоспособного предприятия, в первую очередь, зависит от людей, которые работают на данном предприятии, ведь возможности любой организации напрямую связаны с использованием новых методов управления, а также с конкретными людьми, их знаниями, компетенциями, квалификацией, стрессоустойчивостью, дисциплиной, мотивацией и восприимчивостью к обучению.

Рекомендательные системы – это специальные программы, главная цель которых заключается в формировании рекомендаций различных продуктов или сервисов для пользователей на основе их предпочтений [9].

Рекомендательная система кадровой безопасности предприятия – это программный комплекс, который позволяет проводить оценку и аттестацию персонала с учетом уровня их благонадежности. Программный комплекс состоит из Web-приложения, базы данных и настольной программы для оператора (программа).

Web-приложение позволяет быстро и удобно произвести анкетирование и тестирование пользователей, а также совершает последующую запись этих данных в базу данных.

Программа автоматически обрабатывает пройденные тесты и анкеты новых пользователей и вносит записи результатов в базу данных. Вмешательство оператора при этом необходимо лишь при постановке задачи, которую требуется выполнить, а также для контроля качества работы системы.

Программа отвечает за обработку персональных данных пользователя и пройденных тестов: выбор тестов, которые необходимо пройти каждому пользователю, запись полученных после обработки результатов в базу данных, составление рекомендаций на основе ответов пользователя для оператора программы.

Оператор имеет доступ к данным всех пользователей, зарегистрированных в web-приложения, то есть может посмотреть пройденные тесты, полученный уровень благонадежности, совершённые ошибки в тестах, рекомендации, полученные на основе пройденных тестов, а также оператором могут быть добавлены новые тесты.

Таким образом, рекомендательная система кадровой безопасности предприятия выявляет не только компетенции и поведенческие реакции, но и учитывает требования безопасности сотрудника.

ЛИТЕРАТУРА

1. Искусственный интеллект в подборе персонала [Электронный ресурс]. Режим доступа: <http://confes.fb.tusur.ru/sites/default/files/news/files/confes2017.pdf> (дата обращения: 20.02.2018).
2. Корпоративные компетенции: разработка, развитие, оценка [Электронный ресурс]. – Режим доступа: <https://businessman.ru/korporativnyie-kompetentsii-razrabotka-razvitiie-otsenka.html> (дата обращения: 24.02.2018).
3. Hayes-Roth F., Jacobstein N. Состояние автономных систем. Коммуникации АСМ. (дата обращение: 26.02.2018).
4. SAP HR – программа для управления персоналом [Электронный ресурс]. – Режим доступа: <http://asapcg.com/press-center/articles/sap-hr/> (дата обращения: 20.02.2018).
5. Talent Q [Электронный ресурс]. – Режим доступа: <http://www.talent-q.ru/products> (дата обращения: 26.02.2018).
6. Oracle [Электронный ресурс]. – Режим доступа: <http://www.stud-files.ru/preview/2393324> (дата обращения: 20.02.2018).
7. Роботозамещение [Электронный ресурс]. – Режим доступа: <https://sk.ru/news/b/press/archive/2017/01/16/robotozameschenie.aspx> (дата обращения: 20.02.2018).
8. Харский К.В. Благонадежность и лояльность персонала. – СПб.: Изд. дом «Питер», 2003. – 496 с.
9. Prem Melville and Vikas Sindhwani, Recommender Systems, Encyclopedia of Machine Learning, Claude Sammut and Geoffrey Webb (Eds) [Электронный ресурс]. – Режим доступа: <http://www.prem-melville.com/publications/recommender-systems-eml2010.pdf> (дата обращения: 20.02.2018).

МЕТОДИКА ОЦЕНКИ НА ЭТАПЕ ПОДБОРА ПЕРСОНАЛА В СИСТЕМЕ КАДРОВОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

И.В. Крист, студент, С.В. Глухарева, ст. преп.

*г. Томск, ТУСУР, каф. КИБЭВС, krist-ilya@mail.ru,
samantases@mail.ru*

Современный мир стремительно развивается, это закономерный и динамичный процесс, новые тенденции на рынке труда сменяют друг друга в быстром темпе, тенденции в области управления так же видоизменяются. Изменения происходят в структуре организаций, происходит внедрение автоматизации в рабочий процесс, происходит переход на «цифровую экономику». Непрерывно меняющаяся конъюнктура рынка, высокие скорости в принятии решений, многозадачность в управлении активами и необходимость снижения рисков требуют современных подходов к организации оценки кадров.

Сотрудник является ключевым звеном в функционировании предприятия, набор его компетенций напрямую влияет на кадровую

безопасность предприятия, так как большое количество компетенций позволит по-разному оценивать и устранять угрозу со стороны персонала. Функционирование сотрудника на предприятии начинается с этапа подбора, важно именно на этом этапе, в полной мере оценить кандидата для того, чтобы снизить риски кадровой безопасности.

Процесс подбора персонала имеет свою специфику в каждой организации, нет стандартной методики подбора. Под методикой, в данном случае, понимается пошаговый алгоритм проведения подбора потенциальных сотрудников, при помощи различных инструментов (собеседование, интервью, решение тестов и т.д.).

Этапы подбора во многом зависят от особенностей организации, от специфики должности, на которую подбирается кандидат. Однако в общем виде процесс подбора персонала может быть представлен следующей схемой (рис. 1.):



Рис.1. Обобщенные этапы подбора персонала

Большинство организаций на этапе подбора персонала придерживается представленной выше методики. В ходе оценки обращают внимание на определение лишь личных и профессиональных компетенций. Но для всесторонней оценки необходимо обращать внимание на определение социально-психологических, поведенческих, корпоративных компетенций, компетенций безопасности, успешности и будущего. При оценке кандидатов HR-специалисты ограничиваются использованием тестирования, собеседования, анализа резюме и анкетных данных, что в случае полной оценки компетенций недостаточно. Тесты на профессиональные знания не способны в полной мере оценить владения кандидата профессиональными компетенциями, для оценки следует применять решение кейсов и деловые игры, так как при решении реальных практических задач кандидат показывает свои навыки и умения. Кроме этого, собеседование при оценке кандидата имеет стандартную модель вопросов, проходит достаточно быстро, не позволяя раскрыть основные компетенции потенциального сотрудника. Большинство организаций не использует такой этап как стажиров-

ка кандидата, в ходе которой специалист в рамках решения практических задач показывает уровень владения профессиональными компетенциями в условиях организации.

В рамках кадровой безопасности предприятия разработана методика, включающие следующие этапы:

1) определение потребности в должности. На данном этапе проводится анализ потребности в найме нового специалиста, а также определяется его функционал;

2) составление модели компетенций для должности. На данном этапе составляется перечень необходимых знаний, компетенций, необходимых для качественного выполнения функциональных обязанностей определённой должности;

3) размещение объявления о вакансии. На данном этапе определяются каналы размещения объявлений;

4) телефонное мини-собеседование, на котором проверяется заинтересованность и мотивация кандидата к конкретной должности;

5) анализ представленных резюме кандидатов для проведения первичного отбора кандидатов;

6) анализ заполненных анкет соискателей на сайте компании для сбора информации о кандидате;

7) проведение анкетирования в офисе компании. При заполнении анкеты в офисе компании кандидат оценивается по следующим параметрам: по времени, затраченному на заполнение, грамотности, внимательности, полноте предоставленных данных. На данном этапе оцениваются поведенческие компетенции кандидата в режиме реального времени;

8) проверка рекомендаций и анкетных данных с целью отсева неблагонадежных сотрудников;

9) анализ профиля соискателя в социальных сетях с целью расширения информации о претенденте и составлении его портрета;

10) тестирование. Совокупность тестовых заданий позволит выявить компетенции соискателя для вакантной должности;

11) интервью. В качестве объективной оценки используются несколько видов интервью, таких как стрессовое, компетентностное, личное и др.;

12) решение кейсов, с помощью которых оцениваются профессиональные компетенции;

13) деловые игры. В деловой игре разыгрываются ситуации, которые имитируют производственные условия, которые позволяют выявить как профессиональные, так и поведенческие компетенции;

14) стажировка, которая позволяет оценить соискателя в производственном процессе. После успешного прохождения стажировки

принимается решение о приеме на конкретную должность с испытательным сроком согласно трудовому договору.

Таким образом, преимуществом данной методики оценки персонала на этапе подбора состоит в том, что она позволяет определить уровень благонадежности сотрудника, что в свою очередь позволит выявить недобросовестных и некомпетентных специалистов и обеспечить кадровую безопасность предприятия.

ЛИТЕРАТУРА

1. Соломанидина Т.О. Кадровая безопасность компании: учеб. пособие / Т.О. Соломанидина, В.Г. Соломанидин. – 2-е изд., перераб. и доп. – М.: ИНФРА-М, 2017. – 559 с.
2. Методы подбора персонала [Электронный ресурс]. – Режим доступа: <https://person-agency.ru/research/metod> (дата обращения: 14.02.2018).

ТЕНЕВАЯ ЭКОНОМИКА КАК УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ СТРАНЫ

В.А. Кудрявцева, студентка

Научный руководитель В.В. Жук, ассистент

г. Томск, ТУСУР, каф. КИБЭВС

В абсолютно всех государствах с рыночной экономикой существовала, существует и определённо будет существовать теневая экономика. Масштабы её самые различные, однако, ни одному государству не удастся освободиться от неё совсем. Теневая экономика является основной угрозой экономической безопасности.

В русской научной литературе под теневой экономикой подразумевается весь комплекс финансовой работы, которая никак не учитывается официальной статистикой и никак не вводится в валовый государственный продукт государства, то есть это любая финансовая активность незафиксированная контролирующими органами, например такими, как Федеральная Налоговая служба.

Вопросы теневой экономики стали одними из наиболее значимых, как для Российской Федерации, так и для многих государств нашего мира. Определенные виды теневой деятельности признаны угрозами для национальной экономической безопасности, их включают в состав самых важных проблем нашего времени.

Под экономической безопасностью подразумевается комплекс критериев и условий, которые обеспечивают самостоятельность национальной экономики, ее стабильность и устойчивость, способность к постоянному обновлению и самосовершенствованию. Так же она обеспечивает и гарантирует стабильность финансового формирования

страны и заинтересованность в удовлетворении общественных и экономических потребностей [1].

Теневая экономика – это достаточно не простое общественное экономическое явление, включающая всю концепцию общественно-экономических отношений, и в первую очередь – бесконтрольный обществом раздел воспроизводства, где изготовление, разделение, взаимобмен и потребление финансовых благ и предпринимательских возможностей скрываются от органов управления государством [2].

Теневая экономика представляет собой условие, которое негативно влияет на экономическую безопасность страны. Оптимизация размера теневой экономики в качестве мероприятия единой политики ведёт к увеличению уровня экономической безопасности страны.

К более значимым результатам теневой экономики относятся экономическая преступность и коррупция, которые неизбежно сопровождают теневую экономическую деятельность. Коррупция – это мощное условие, которое ограничивает увеличение уровня экономической безопасности и производит неэффективное применение ресурсов.

Причинами теневой экономики является возникновение противоречий среди повышенных потребностей субъектов хозяйствования и малыми возможностями легального социального производства. Так, по данным опубликованным на сайте РБК, в 2016 году Россия вошла в пятерку самых крупных теневых экономик, она заняла четвертое место в рейтинге, в который включены 28 стран. Её объем составляет 33,6 трлн руб., или 39% от прошлогоднего ВВП страны [3].

Классификация теневой экономики представлена на рис. 1, она подразделяется на два вида экономики: криминальную и вынужденную нелегальную.

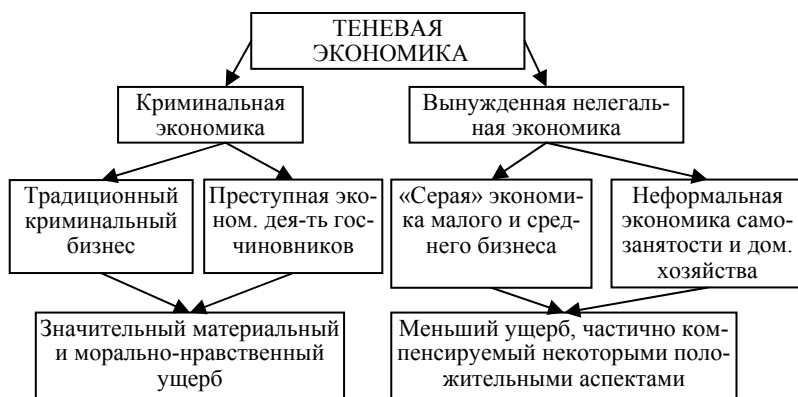


Рис. 1. Классификация теневой экономики

Так как движения теневой экономики затрагивают в какой-то степени большинство отраслей экономики, то исследование собранного теоретического и практического навыка и конфигурирования оптимизации её посредством призмы экономической безопасности является очень актуальным.

Доказано, что целиком и полностью ликвидировать нелегальный (теневой) бизнес нельзя. Если существует открытая экономика в стране, то будет существовать и скрытая экономика. К счастью, можно снизить объёмы теневой экономики. Однако для достижения этой цели необходимо постоянно долговременно и целенаправленно работать в заданном направлении. В отношении нелегальной экономики необходимы два типа действий. С одной стороны, с теневой экономикой предстоит бороться, а это функции налоговых и правоохранительных органов, и они обязаны выполнять их, как можно лучше. Со второй стороны необходимо привести скрытую деятельность к стандартным масштабам с помощью полной легализации, только таким образом, чтобы всё это шло в пользу экономике страны [4].

Для снижения объема теневой экономики нужны значительные перемены в экономико-политической деятельности государства, изменение законодательства и искоренение мнения о безнаказанности осуществления предпринимательской деятельности вне рамок законодательства.

ЛИТЕРАТУРА

1. Грунин О., Грунин С. Экономическая безопасность организации – СПб.: Питер, 2010. – 26 с.
2. Понятие, виды и формы теневой экономики [Электронный ресурс]. – Режим доступа: <http://www.grandars.ru/student/nac-ekonomika/vidy-tenevoy-ekonomiki.html> (дата обращения: 25.02.2018).
3. Россия вошла в пятерку стран с крупнейшей теневой экономикой [Электронный ресурс]. – Режим доступа: <http://www.rbc.ru/economics/30/06/2017/595649079a79470e968e7bff> (дата обращения: 26.02.2018).
4. Влияние теневой экономики на обеспечение экономической безопасности [Электронный ресурс]. – Режим доступа: <http://www.m-economy.ru/art.php?nArtId=2107> (дата обращения: 01.03.2018).

БЛОКЧЕЙН КАК ПОМОЩНИК В ОБЕСПЕЧЕНИИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

М.О. Мамскова, студентка

*Научный руководитель Е.И. Губин, доцент каф. КИБЭВС
г. Томск ТУСУР, каф. КИБЭВС, g_ei@mail.ru*

Опыт показывает, что компании или люди, которые раньше начинают использовать революционные технологии, больше других от них и выигрывают. Это утверждение заслужено и в отношении развивающейся технологии под названием блокчейн.

Блокчейн – распределенная база данных, которая хранит информацию обо всех транзакциях участников системы в виде криптографической «цепочки блоков» (именно так с англ. переводится Blockchain). Доступ к реестру есть у всех пользователей блокчейна, выступающих в качестве коллективного нотариуса, который подтверждает истинность информации в базе данных. Блокчейн может применяться для финансовых операций, идентификации пользователей, создания технологий кибербезопасности и др. [1].

Технология блокчейн действительно можно назвать революционной, ведь она предлагает совершенно новые способы взаимодействия между компаниями и людьми, увеличивая при этом скорость передаваемой информации, ее защиту, исключая посредников и установление более доверительных отношений. Вот почему технология блокчейн так заинтересовала профессиональные, научные круги и правительства во всем мире.

Принято считать, что появление блокчейн-технологии связано с первой криптовалютой которая появилась в 2008 году (во время разгара всемирного финансового кризиса). Однако Ассе Сауга (один из первых профессионалов по блокчейн-технологии из банковского сектора) утверждает, что многие проекты с блокчейном были разработаны в 1990-х годах. Все они работали в виде централизованной системы транзакций, а с появлением криптовалюты Bitcoin произошло первое применение децентрализованной блокчейн-технологии [2]. Это так же свидетельствует о том, что возможности применения данной технологии выходят далеко за границы цифровой сферы в физический мир и могут оказать реальное воздействие на все аспекты экономики.

Блокчейн заменяет устаревшие и ограничивающие методы ведения бизнеса – «помехи», которые тормозят более легкое и эффективное сотрудничество компаний. Благодаря надежному распределенному реестру, защищенному новейшими технологиями шифрования и проверки данных. Допущенная сеть участников охраняет целостность

реестра, при этом каждая сторона может вносить изменения и видеть только ту информацию, к которой у нее есть доступ в рамках транзакции. Данные всех транзакций неизменно сохраняются в реестре, это означает, что никто не сможет переписывать или отрицать историю. Следовательно, уйдет утверждение «правда у каждого своя», а в любых спорных вопросах будут рассматриваться реальные факты.

Иными словами, блокчейн исключает возможность мошенничества, потому что все данные открыты для участников и лиц, имеющих доступ. Риск сведен к минимуму в системе, в которой управление по сути распределено между участниками. Это и есть эталонное определение доверия [3].

Хочется показать на примере, как технология блокчейн сможет оптимизировать бизнес процессы в реальной жизни и облегчит обеспечение экономической безопасности в компании. Возьмем для примера одну из сфер, в которой технология блокчейн смогла бы упростить взаимодействие между контрагентами, эта сфера сейчас является наиболее проблемной для сотрудничества сфера международной торговли.

Представьте, в России существует компания по продаже бытовой техники, закупку электроприборов они производят от поставщика, который находится в Китае. На закупку российская компания берет кредит в банке и с этих средств осуществляет лишь предоплату по договору. Затем, приборы проходят транспортировку из одной страны в другую, проходя таможенные посты двух стран, пользуясь одной или несколькими транспортными компаниями. После получения товара владелец магазина должен подтвердить банку, что сделка осуществлена, и происходит окончательный перевод суммы поставщику. Этот процесс мало изменился за последние столетия, он порождает существование посредников, уязвимых мест для мошенничества и потерю времени. Но что, если данный процесс оптимизировать с помощью технологии блокчейн, где вся информация находится в свободном доступе и наглядно происходит изменение, так еще с помощью умных контрактов условия договора могут выполняться автоматически.

Хочется сделать небольшое отступление и пояснить, что означают умные контракты или smart контракты. Смарт-контракты, так называются сделки и другие договоры, которые заключаются полностью в цифровом виде, а их исполнение (например, переход права собственности от одного владельца к другому) обеспечивают компьютерные протоколы без участия человека. То есть протоколы автоматически проверяют возможность и законность сделки; они не допускают

заклучение договора, если его условия не удовлетворяют установленным нормам [3].

Упрощенно говоря – это контракты, которые проверяют и исполняют себя сами, т.е. если у человека на счету не будет нужной суммы заплатить за вашу услугу, смарт-контракт проверит это заранее и не позволит совершиться такой сделке.

В smart-контракте может быть указано, что, когда товары достигнут определенный пункт назначения и таможенные органы разрешат их ввоз, деньги автоматически переводятся из банка получателя в банк отправителя – без задержек, рассмотрения и периода ожидания. Эти контракты находятся в блокчейн, при этом участники сделки видят и подписывают только ту часть, которая относится к их стороне.

Появившиеся новые возможности позволяют переосмыслить всю систему ведения бизнеса, поскольку выполнение многих договорных обязательств происходит посредством программного кода, что минимизирует вероятность появления человеческой ошибки, оплошности. Благодаря существованию единственного достоверного варианта в реестре, расходы на проверку потенциальных партнеров резко сократятся, многие споры перестанут возникать, а круг участников экономического процесса резко расширится.

С блокчейном необходимость ручного следования правилу «доверяй, но проверяй» и все связанные с этим затраты уйдут в прошлое. В этой ситуации в принципе исключается наличие ненадежных контрагентов, ведь подменить данные или приукрасить свою финансовую историю будет невозможно, все документы будут зашифрованы и резервно скопированы, ситуация с потерей или подделкой документа становится не возможной.

Преимущества блокчейна уже изучаются многими организациями, которые понимают невероятный потенциал этой технологии.

Например, ретейлер Overstock получил разрешение от властей использовать технологию блокчейна для международного размещения, оплаты и торговли корпоративными облигациями.

В Эстонии в сотрудничестве с NASDAQ предлагается услуга электронного голосования, основанная на технологии блокчейна, которая позволяет акционерам компаний, торгующихся на Таллинской фондовой бирже (входит в группу NASDAQ), голосовать на собраниях акционеров.

IBM совместно с Лондонской и Токийской фондовыми биржами тестирует применение блокчейна для торговли на рынках с низкой ликвидностью [3].

Правительство Швеции, вынесло решение переводить земельный кадастр на блокчейн [4].

Конечно такая технология не может не привлекать внимание, так «За 2012–2016 гг. было вложено в технологию порядка \$1,4 млрд, а в 2017 г. банки планировали инвестировать уже до \$1 млрд в распределенные реестры, по данным Ernst & Young. Оценка экономии со стороны банков при использовании технологии блокчейн составляет порядка \$20 млрд. «8% из 3000 опрошенных организаций в разных странах мира перешли на пилотную или реализационную стадию внедрения блокчейна. 25% в настоящее время изучают возможности реализации в ближайшее время. Среди них финансовые компании 33%, правительственный сектор 29%, здравоохранение 27%», – Кириакос Коккинос, исполнительный директор, партнер IBM Europe.

Блокчейн сокращает расходы, снижает риски, способствует возникновению новых бизнес-моделей и повышает эффективность сделок. Эта технология значительно расширит доступ на международный рынок для новых участников. Тех, кто готов внедрить эту передовую технологию, ожидает действительно успешное будущее. [3] такого же мнения придерживается и основатель Movencorp Inc – Бретт Кинг: «Блокчейн – это революция в плане структурного воздействия на банковскую сферу» [5].

Как бы революционно это ни звучало, блокчейн действительно представляет собой механизм, обеспечивающий высшую степень учета и идентификации. Больше не будет пропущенных транзакций, ошибок человека или машины, или даже изменений, сделанных без согласия вовлеченных сторон. А наиболее важно то, что блокчейн помогает гарантировать законность транзакции путем записи её не только в главном реестре, а в распределённой системе реестров, связанных через защищенный механизм проверки [4]. Блокчейн сокращает расходы, снижает риски, способствует возникновению новых бизнес-моделей и повышает эффективность сделок. Данная технология действительно расширяет возможности компаний это означает что обеспечение экономической безопасности в организации или финансовой сфере, станет проще, эффективнее и приведет к минимизации угроз. Конечно на ряду с многочисленными плюсами существуют и минусы, такие как отсутствие законодательной базы, нужны большие финансовые вложения для перестройки уже устоявшихся систем, большие затраты электроэнергии и т.д. но, если бы человек боялся сделать шаг вперед на встречу неизвестному мы бы просто остановились в развитии, ведь шаг вперед это всегда шаг за грань привычного, обыденного и не изведенного. Не стоит забывать, что и интернет был, когда-то новым, чужеродным и непознанным, а сейчас уже трудно представить жизнь без него. Так может данная технология это и есть новый шаг за горизонт.

ЛИТЕРАТУРА

1. «Технология блокчейн. То, что движет финансовой революцией сегодня». Алекс и Дон Тапскотт <http://www.the-village.ru/village/weekend/books/285328-kniga> (дата обращения: 01.03.2018).
2. [Электронный ресурс]. – Режим доступа: <https://xn-80adhipggue3h8a.xn--p1ai/tekhnologii/blokcheyn/blokcheyn-bitcoin-kto-pervyy/> (дата обращения: 09.03.2018).
3. IBM [Электронный ресурс]. – Режим доступа: <http://cognitive.rbc.ru/blockchain/> (дата обращения: 05.03.2018).
3. Rubase [Электронный ресурс]. – Режим доступа: <https://rb.ru/opinion/blockchain/> (дата обращения: 08.03.2018).
4. «TADVISER» деловой портал [Электронный ресурс]. – Режим доступа: <http://www.tadviser.ru/index.php/> (дата обращения: 06.03.2018).
5. Блокчейн – рождение новой экономики [Электронный ресурс]. – Режим доступа: <http://tass.ru/pmef-2017/articles/4309321> (дата обращения: 12.03.2018).
6. Что такое блокчейн [Электронный ресурс]. – Режим доступа: <https://mining-cryptocurrency.ru/blockchain/> (дата обращения: 09.03.2018).

УГРОЗА ОТКЛЮЧЕНИЯ РОССИЙСКИХ ОРГАНИЗАЦИЙ ОТ СИСТЕМЫ SWIFT. ПЕРСПЕКТИВЫ РАЗВИТИЯ СИТУАЦИИ

Н.Н. Манчилаева, студент

*Научный руководитель О.В. Кочетков, преп. каф. КИБЭВС
г. Томск, ТУСУР, каф. КИБЭВС, manchilaewa@mail.ru*

На сегодняшний день совершение международных платежей и передача финансовой информации является серьезной проблемой для российских банковских организаций, это связано с ведением секторальных санкций Евросоюза и США по отношению к России, которые в свою очередь могут повлиять на отключение российских организаций от платежной системы SWIFT (от англ. Society for Worldwide Interbank Financial Telecommunications).

Данная проблема является актуальной, так как в настоящее время создание единой национальной инфраструктуры обмена финансовыми сообщениями напрямую связана с обеспечением национальной экономической безопасности страны.

На данный момент российские банковские организации пользуются услугами международной платежной системы SWIFT. Система охватывает более тысячи финансовых организаций по всему миру. Ежедневно через систему SWIFT проходят платежные поручения на сумму более шести триллионов долларов. За день в России отправляется через систему SWIFT около 360 тысяч сообщений. При подклю-

чении к системе SWIFT российские пользователи получают услуги, которые включают в себя быструю, надежную и высокоэффективную организацию передачи информации.

Отключение от международной системы SWIFT создаст немалые сложности, в первую очередь возникнет проблема для двусторонних банковских сообщений при осуществлении платежей как внутри России, так и за рубежом.

Исследуя проблему, отключения российских банковских организаций от международной системы SWIFT, стоит проанализировать финансовые потери, которые могут ожидать российские банковские организации. Для начала рассмотрим количество пользователей SWIFT, а также стоимость услуг, предоставляемых крупнейшими пользователями системы SWIFT в России.

На 1 января 2017 г. в России было зарегистрировано 436 пользователей SWIFT, включающих финансовые учреждения и корпорации. По количеству пользователей SWIFT наша страна занимает второе место в мире, уступая по данному показателю США. В среднем в России стоимость передачи одного международного сообщения через систему SWIFT составляет 17,31 евро центов [1].

Рассмотрим на примере Банка России, стоимость услуги по передаче финансовых сообщений в формате SWIFT, которая осуществляется в соответствии с показателями (см. табл. 1) [2].

Т а б л и ц а 1

Тариф на услугу Банка России по передаче финансовых сообщений в формате SWIFT

Количество финансовых сообщений в формате SWIFT, направляемых участникам обмена (ежедневно)	Тариф на услугу Банка России по передаче финансовых сообщений в формате SWIFT (за одно финансовое сообщение)
От 1 до 300	2 руб. 50 коп.
От 301 до 500	2 руб.
Свыше 500	1 руб. 50 коп.

Кроме тарифов Банка России взимаются комиссии за переводы. В табл. 2 показаны одни из популярных российских банков, предоставляющие данную услугу.

Исходя из приведенных данных можно сделать вывод о том, что при отключении системы SWIFT, у российских организаций произойдет снижение прибыли от предоставляемых услуг, связанных с международными переводами.

В марте 2017 г. председатель Банка России Эльвира Набиуллина на встрече с президентом Владимиром Путиным заявила, что россий-

ская финансовая система защищена на случай отключения от системы SWIFT и международных платежных систем. Она пояснила, в России создан аналог SWIFT. Он получил название «Система передачи финансовых сообщений» (СПФС) [3].

Таблица 2

Комиссии за международный перевод по системе SWIFT

Банковская организация	Комиссия за перевод, % от Σ (min, max)	
	При наличии счета	Без открытия счета
Сбербанк России	1% (15–200 долл. США)	2% (50–1500 руб.)
Альфа Банк	0,5–2% (750 – 8000 руб.)	Не проводится
Райффайзенбанк	1,5% (30 – 250 долл. США)	Не проводится

Система передачи финансовых сообщений (СПФС) – функционирующая на базе информационно – телекоммуникационной системы Банка России, создана в качестве альтернативного канала межбанковского взаимодействия с целью обеспечения гарантированного и бесперебойного предоставления услуг по передаче электронных сообщений по финансовым операциям.

Функции СПФС:

- передача сообщений формата SWIFT;
- передача сообщений в собственных форматах пользователей;
- контроль финансовых сообщений формата SWIFT [4].

Несмотря на то что в банковскую систему России была введена система передачи финансовых сообщений, на данный момент платежная система СПФС имеет свои недочеты она не может в полном объеме осуществлять международные банковские операции, а также система имеет высокую стоимость сообщения и низкую скорость передачи информации.

В случае отключения от SWIFT, у банковской системы России есть вариант сотрудничества с международными банками-контрагентами, но и этот вариант является не выгодным для России так как при взаимодействии с банками увеличится стоимость передачи информации и увеличится время на процесс перевода.

На данный момент данные альтернативные варианты являются недостаточно эффективными для выхода из возможной ситуации, тем самым можно сделать вывод о том, созданная платежная система СПФС имеет большие перспективы в развитии передачи телекомму-

никационных сообщений, для того, чтобы она полностью заменила международную систему SWIFT, необходимо до конца проработать реализацию системы, исправить имеющиеся недочеты и в дальнейшем разработать возможность передачи сообщений в международном формате, чтобы при отключении системы SWIFT, в Российской банковской системе не произошел экономический коллапс.

ЛИТЕРАТУРА

1. Официальный портал Российской Национальной Ассоциации SWIFT [Электронный ресурс]. – Режим доступа: <https://russwift.ru/300> (дата обращения: 27.02.2018).
2. Официальный сайт Центрального банка РФ [Электронный ресурс]. – Режим доступа: <http://www.cbr.ru/psystem> (дата обращения: 27.02.2018).
3. Экономический портал «Русская весна» [Электронный ресурс]. – Режим доступа: <http://rusvesna.su/economy> (дата обращения: 27.02.2018).
4. Официальный сайт Центрального банка РФ [Электронный ресурс]. – Режим доступа: <http://www.cbr.ru> (дата обращения 27.02.2018).

МЕТОД АНКЕТИРОВАНИЯ НА ЭТАПЕ ПОДБОРА ПЕРСОНАЛА В СИСТЕМЕ КАДРОВОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Е.В. Мареева, студентка

*Научный руководитель С.В. Глухарева, ст. преп. каф. КИБЭВС
г. Томск, ТУСУР, каф. КИБЕВС, gsv@keva.tusur.ru
Проект ГПО КИБЭВС-1517 «Система кадровой
безопасности предприятия»*

Известно, что «сотрудник является не только основным активом компании, но и главным источником угроз для любой организации. Следовательно, обеспечение комплекса мер по предотвращению рисков, связанных с людьми и их профессиональной деятельностью, является одной из главных задач» [1]. Именно сотрудник составляет основу кадровой безопасности предприятия.

Система кадровой безопасности предприятия предполагает комплексный подход к оценке персонала, в том числе и кандидата на ту или иную должность. Для того, чтобы оценить в полном мере кандидата, необходимо собрать о нем как можно больше информации. Инструментом сбора информации служит анкета. Анкета – это «не механическая последовательность вопросов, которые располагаются в ней в зависимости только от личного желания исследователя, а определённая взаимосвязь вопросов, образующих особое целое» [2].

С 1920 г. наибольшее внимание уделялось развитию и более глубокому анализу метода анкетирования [3]. В настоящее время, данный метод используется во всех сферах деятельности для переработки, сравнения, осмысления и исследования полученной информации [3, 4]. В большинстве случаев, анкетирование на этапе подбора применяется с целью сбора необходимой информации о потенциальном сотруднике, которая включает такие данные как: паспортные данные, контактная информация, сведения о месте жительства и регистрации, семейное положение и родственные связи, наличие детей, сведения об образовании, сведения об опыте и стаже работы, контактная информация представителей с прошлого места работы.

В настоящее время, в рамках кадровой безопасности предприятия, метод анкетирования представляет собой «сложную и трудоемкую аналитическую работу, целью которой является отражение требований компании, изучение фактических данных будущего сотрудника, его психологические особенности, способность предсказать его реакцию на вопросы, обнаружить степень его честности и искренности при прохождении анкетирования, так как достоверность предоставленной информации соискателем играет важную роль в обеспечении кадровой безопасности предприятия» [1, 2, 5].

Фактическая информация о будущем сотруднике является обязательной частью содержания любой анкеты и наличие ответов на данные вопросы способствуют сбору информации о личности соискателя. Для более глубокого анализа, в рамках кадровой безопасности предприятия, наличие только вышеуказанных вопросов будет недостаточно, так как «фактические данные предоставляют основную информацию о претенденте и не требуют от него развернутого ответа, что является значительной преградой при составлении полного портрета личности потенциального сотрудника» [1, 5]. Для повышения эффективности деятельности компании и снижения рисков, возникающие в связи с некомпетентностью персонала и недоброкачественной работой, для каждой компании необходима любая дополнительная информация, которую необходимо проанализировать и переработать. Следовательно, анкета при трудоустройстве должна содержать перечень как фактических, так и дополнительных вопросов, которые требуют от претендента развернутого ответа, что позволяет составить полный портрет личности соискателя и определить уровень его профессионализма.

Анкетирование должно быть составлено таким образом, чтобы её «блоки включали в себя перечень закрытых и открытых вопросов, с целью сбора полной информации о личности претендента и уровне

его компетентности, за счёт изучения фактических данных и аргументации дополнительных ответов на вопросы» [1, 2, 5]. Дополнительная информация (информация о дополнительном образовании, знании иностранного языка, водительские права, подробная информация о семейном положении, стаже и опыте работы) способствует провести качественный анализ претендента, который в рамках кадровой безопасности, позволяет на этапе анкетирования определить начальный уровень благонадёжности. Метод анкетирования является всего лишь первым этапом, который позволит отсеять неблагонадёжных сотрудников и выбрать тех, которые с помощью тестирований будут проходить дальнейшую проверку на следующем этапе.

Таким образом, информация о будущем сотруднике и ее качественный анализ играет важную роль в рамках кадровой безопасности предприятия. Разработанный метод анкетирования, позволяет принять верное управленческое решение и выбрать сотрудника с высоким уровнем благонадёжности.

ЛИТЕРАТУРА

1. Кадровая безопасность [Электронный ресурс]. – Режим доступа: <https://www.hr-director.ru/article/66809-qqq-17-m8-kadrovaya-bezopasnost-obespechenie-sozdanie> (дата обращения: 17.02.2018).
2. Методика и техника составления анкеты. [Электронный ресурс]. – Режим доступа: <http://refleader.ru/jgebewujgpolyfs.html> (дата обращения: 17.02.2018).
3. История и развитие маркетинговых исследований. [Электронный ресурс]. – Режим доступа: <http://coolbusinessideas.info/istoriya-marketingovyh-issledovaniy/> (дата обращения: 18.02.2018).
4. Онлайн анкетирование как способ исследования [Электронный ресурс]. – Режим доступа: <http://works.doklad.ru/view/M1oxQ3uJLRM.html> (дата обращения: 25.02.2018).
5. Анкетирование при приёме на работу – взгляд со всех сторон [Электронный ресурс]. – Режим доступа: <http://hr-portal.ru/article/anketirovanie-pri-prieme-na-rabotu-vzglyad-so-vseh-storon> (дата обращения: 01.03.2018).

ОЦЕНКА ЭФФЕКТИВНОСТИ ВЫПОЛНЕНИЯ АДРЕСНЫХ ПРОГРАММ ЖКХ ПО ПРОВЕДЕНИЮ КАПИТАЛЬНОГО РЕМОНТА В МНОГОКВАРТИРНЫХ ДОМАХ

О.И. Маркова, аспирант каф. КИБЭВС

г. Томск, ТУСУР, markovaolgatusur@gmail.com

ЖКХ – занимает ключевую роль в экономики субъектов и государства в целом, что говорит о важности модернизации данной отрасли и ведение такого механизма, который сможет сделать всю систему

открытой и доступной для граждан России. Что выявляет необходимость быстрого перехода на традиционные (рыночные) методы ведения хозяйства.

На протяжении нескольких лет, вопрос о правильности и эффективности распределения средств долевого финансирования в сфере жилищного коммунального хозяйства (далее – ЖКХ) волнует большое количество граждан. Сфера ЖКХ является одной из наиболее финансируемых отраслей социальной политики, как со стороны государства, так и со стороны граждан, в виде отчислений за капитальный ремонт в Фонд ЖКХ. Финансирование программ ЖКХ в 2015–2017 гг. составило 1 225 млрд. руб. Из этих средств 771 млрд. руб. направлено на реализацию программ по проведению капитального ремонта МКД (смотреть рис. 1) [1].

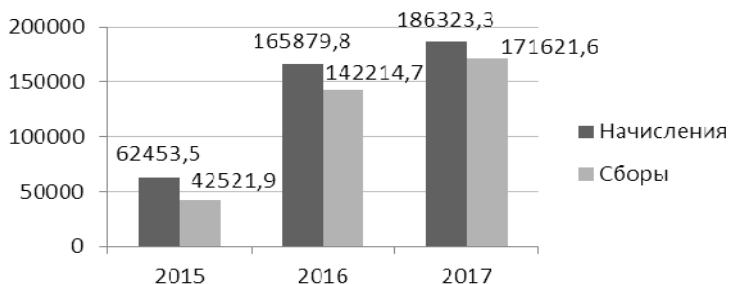


Рис. 1. Выделение средств на проведения капитального ремонта МКД в период с 2015 по 2017 гг.

Согласно ГОСТ Р 56193–2014 ежегодный объем ремонтируемых МКД должен быть не менее 4 % общей площади жилищного фонда. Однако общее число МКД в России, которые находятся на стадии износа – в среднем составляет 48,3%, согласно данным Росстата, что в свою очередь занимает 2154322 ед., в указанных МКД проживает более 61 млн. человек [2].

Как видно на рис. 2 наибольший износ зафиксирован в Курской области – 100% износа, Магаданская область – 90,36%, Новгородской области – 90,32%, Тульская область – 84,31%, Республика Крым – 83,05%, Республика Коми – 82,95%. Наименьший износ или отсутствие износа зданий зафиксирован в Мурманской, Ленинградской, Смоленской, Ростовской, Астраханской и Курганской областях, в данных областях процент износа равен или близок к нулю.

В свою очередь доля включения МКД в региональные программы капитального ремонта составляет менее 35%, а именно 737 тыс. ед. и

еще 65,8% остаются не включенными в программу – 1,4 млн. ед. (рис. 2).

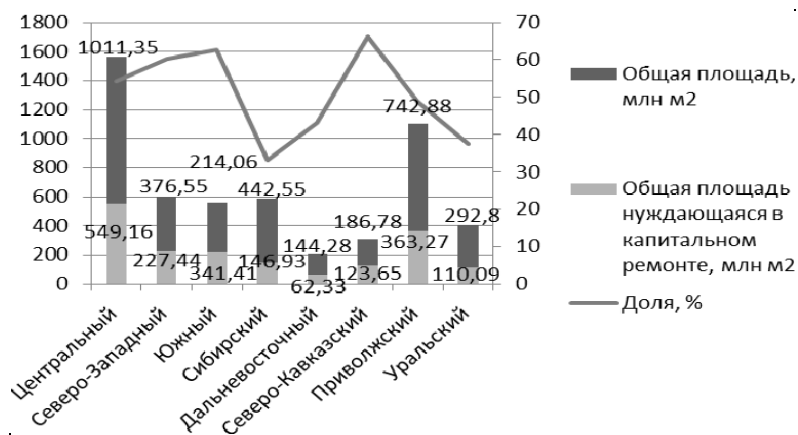


Рис. 2. Значения жилищного фонда, нуждающиеся в проведении капитального ремонта, в разрезе федеральных округов

Основные нарушения выполнения адресных программ по капитальному ремонту МКД жилищного фонда [4]:

1. Перечисление авансовых платежей (теневых), которые превышают предусмотренные нормативы (30%) – 213 925,7 тыс. руб., или 2,1%.
2. В нарушение ч. 11 ст. 20.1 Федерального закона № 185-ФЗ – оплата работ и услуг по капитальному ремонту, не согласованных с органами местного самоуправления.
3. Невыполнение экспертизы сметной документации.
4. Нарушение технических регламентов и строительных норм и правил.

ЛИТЕРАТУРА

1. Суринов А.Е. Россия в цифрах.: Крат. стат. сб. – М.: Росстат, Р76. – 2017. – 511 с.
2. Суринов А.Е. Российский статистический ежегодник: Стат. сб. – М.: Росстат, Р76. – 2017. – 686 с
3. Егоренко С.Н. Регионы России. Социально-экономические показатели: Стат. сб. – М.: Росстат, Р32. – 2017. – 1402 с.
4. Жилищное хозяйство в России. М.: Росстат, 2016 [Электронный ресурс]. – Режим доступа: http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/population/housing/ (дата обращения: 01.03.2018).

ВЛИЯНИЕ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ ТОМСКОЙ ОБЛАСТИ

П.Н. Орлихина, студентка

Научный руководитель А.А. Конев, доцент, к.т.н.

г. Томск, ТУСУР, каф. КИБЭВС, polina_orlihina@mail.ru

Чрезвычайные ситуации по своей природе оказывают воздействие на все сферы существования человеческого общества и главным образом на природную среду и жизнедеятельность людей.

Обеспечение безопасности населения, территорий и объектов экономики в зоне ЧС, за счёт экономического обеспечения данных мероприятий является основным элементом по предупреждению и ликвидации последствий чрезвычайных ситуаций и данному аспекту в наши дни уделяется большое внимание. Поэтому досрочное прогнозирование экономических последствий от чрезвычайных ситуаций, можно считать основной задачей в данном вопросе, поскольку оно является правильным при формировании и своевременном осуществлении защиты объектов экономики, населения, территорий от ЧС экономическими механизмами. Данные действия способствуют значительному снижению социально-экономического ущерба и повышению уровня безопасности, за счёт использования материально-технических ресурсов и ограниченных финансовых ресурсов.

На данный момент в России ежегодный прямой экономический ущерб от чрезвычайных ситуаций оценивается в 4–5% от ВВП, в особо тяжелых случаях может достигать 10% [1]. Триллионами рублей в год исчисляется рост прогнозируемого количества возникающих чрезвычайных ситуаций различного характера, а также ущерба от них, что существенно замедляет экономический рост в государстве и замедляет процесс перехода России к стратегии устойчивого развития. По исследованиям МЧС России ущерб от последствий чрезвычайных ситуаций и природных бедствий во много раз больше, чем возможности мирового сообщества в оказании гуманитарной помощи пострадавшим [2]. С каждым годом данная проблема становится все больше и больше и приобретает глобальный характер.

Ущерб и потери от чрезвычайных ситуаций являются основными составными частями, которые учитывают тяжесть последствий. Ущерб представляет собой материальный и финансовый урон, понесенный в процессе чрезвычайной ситуации.

Экономический ущерб представляет собой выраженную в процентах стоимости объекта или денежных единицах величину размера негативных экономических последствий от чрезвычайных ситуаций.

В Российской Федерации в связи с этим приобрела общенациональную значимость деятельности по прогнозированию и предупреждению чрезвычайных ситуаций, она же является одной из сфер национальной безопасности страны, поднятой на уровень государственной политики.

Данное положение дел обязывает просчитывать возможный экономический ущерб от предполагаемых чрезвычайных ситуаций при разработке государственной экономической политике, планировании бюджетов, прогнозов социально-экономического развития страны и макроэкономических программ.

Для определения соотношения экономического ущерба от чрезвычайных ситуаций в Томской области и планирования бюджета Томской области были изучены статистические сведения о ЧС, пожарах и их последствиях в Томской области [3]. Также изучен прогноз чрезвычайной обстановки на территории Российской Федерации на 2017 г., данные по законам Томской области об областных бюджетах за 2014–2017 г. и законы Томской области «об исполнении областного бюджета» за 2014–2017 гг. [4–8].

Изучив данные документы было выявлено что отсутствует четкая картина чрезвычайных ситуаций, произошедших за фактический период, так как отсутствуют данные об этих ЧС за определенный период; суммы на плановые два года при составлении бюджета на фактический период всегда равны и значительно меньше необходимых; планируемые суммы по строкам бюджета направленные на предотвращение, ликвидацию чрезвычайных ситуаций и работу органов по предотвращению и ликвидации ЧС в конечном итоге расходуются не полностью, процент исполнения бюджета обычно 90–93%, что говорит о том, что при составлении бюджета на планируемый период, следует тщательнее учитывать затрачиваемые средства.

ЛИТЕРАТУРА

1. Официальный сайт Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий [Электронный ресурс]. – Режим доступа: <http://www.mchs.gov.ru/> (дата обращения: 21.11.2017).
2. Прогноз чрезвычайной обстановки на территории Российской Федерации на 2017 год. – Москва, 2016 [Электронный ресурс]. – Режим доступа: http://www.mchs.gov.ru/upload/site1/Prognoz_na_2017_god_gotovyy.pdf (дата обращения: 21.11.2017).
3. Официальный сайт Главного управления МЧС России по Томской области [Электронный ресурс]. – Режим доступа: <http://70.mchs.gov.ru/> (дата обращения: 21.11.2017).

4. Об областном бюджете на 2014 год и на плановый период 2015 и 2016 гг.: Закон Томской области от 27 декабря 2013 г. №227-ОЗ [Электронный ресурс]. – Режим доступа: <https://duma.tomsk.ru/upload/files/zakonodatelstvo/227-oz.pdf> (дата обращения: 20.09.2017).

5. Об областном бюджете на 2015 год и на плановый период 2016 и 2017 годов: Закон Томской области от 23 декабря 2014 №2421 [Электронный ресурс]. – Режим доступа: https://duma.tomsk.ru/upload/files/zakonodatelstvo/29333_budget2015.pdf (дата обращения: 02.10.2017).

6. Об областном бюджете на 2016 год и на плановый период 2017 и 2018 годов: Закон Томской области от 24 декабря 2015 №3012 [Электронный ресурс]. – Режим доступа: https://duma.tomsk.ru/upload/files/bud16_18.pdf (дата обращения: 10.10.2017).

7. Об областном бюджете на 2017 год и на плановый период 2018 и 2019 годов: Закон Томской области от 29 декабря 2016 №174-ОЗ [Электронный ресурс]. – Режим доступа: <https://duma.tomsk.ru/upload/files/174.pdf> (дата обращения: 20.10.2017).

8. Об исполнении областного бюджета за 2015 год: Закон Томской области от 30 июня 2016 №3315 [Электронный ресурс]. – Режим доступа: https://duma.tomsk.ru/upload/files/77_2015.pdf (дата обращения: 30.10.2017).

БЛОКЧЕЙН В ЦИФРОВОЙ ЭКОНОМИКЕ: ПРЕИМУЩЕСТВА И ПРОБЛЕМЫ

Н.В. Петрова, студентка

*Научный руководитель Е.Г. Алдохина, ст. преп. каф. КИБЭВС
г. Томск, ТУСУР, nadezhda-petrova-1997@mail.ru*

Экономическая безопасность финансовых активов в настоящее время является одной из главных задач государства. Для ее реализации необходимо совершенствование технологий защиты данных. Сможет ли криптовалюта, основанная на блокчейн-технологии обезопасить денежные средства от хакеров? Исследователи в области кибер-безопасности оценивают ущерб от атак мошенников в размере до триллиона долларов. Цель хакеров – кража денежных средств с электронных кошельков, со счетов банков, государственных учреждений и крупных холдингов. Вероятно, поэтому сейчас так быстро набирает популярность платежная единица в виде программного кода [1].

Ее преимущества позволяют конкурировать с другими платежными средствами:

- высокая защищенность от хакинга;
- полный контроль пользователем своих данных;
- минимальная комиссия за транзакции.

Наличие всех этих качеств достигается благодаря технологии блокчейн. Ее развитие началось с появления биткойнов в 2008 г. На простом языке «биткойн» – это виртуальная валюта, с помощью которой можно совершать транзакции – оплачивать покупки, делать переводы, обменивать электронные деньги на наличные и т.д. [2].

Блокчейн – это огромная база данных, которой могут пользоваться все без исключения. В ней нет централизованного руководства. Главными участниками выступают майнеры. Они проверяют различные сделки и транзакции. Если в ходе проверки не было выявлено нарушений, то майнер создает и формирует блоки, которые затем выстраиваются в общую цепочку. Это происходит за счет сложных математических алгоритмов. Хешированием, т.е. процессом преобразования данных, занимаются компьютеры. При получении одинаковых расчетов, блоку присваивается уникальная цифровая подпись. Этот блок больше никогда не может быть изменен. Таким образом, риск мошенничества сводится к нулю.

Главный плюс технологии перед транзакциями банков – отсутствие посредников. Аналитики выдвигают предположение о том, что блокчейн вскоре заменит декларирование, сертификацию и лицензирование.

В книге «Блокчейн. Схема новой экономики», основатель института блокчейн-исследований, Мелани Свон выделяет три основные области применения данной технологии:

1. Blockchain 1.0 – это валюта (криптовалюты применяются в разных приложениях, которые имеют отношение к финансовым транзакциям, например системы переводов и цифровых платежей).

2. Blockchain 2.0 – это контракты (приложения в области экономики, рынков и финансов).

3. Blockchain 3.0 – приложения, область которых выходит за рамки финансовых транзакций (здравоохранение, наука и др.).

Различные примеры первых проработок использования приложений, представлены в таблице [3].

Технология блокчейн не до конца усовершенствована. Вследствие чего существует ряд проблем:

- отсутствие государственного регулирования выпуска криптовалюты. Правовой статус системы значительно различается в разных странах;

- недостаточная массовая грамотность. Технология предполагает распространение на широкие слои населения. Нужно решить вопросы, связанные с конфиденциальностью и безопасностью;

- проблема идентификации пользователей. В настоящее время банки занимаются вопросами идентификации. Через несколько лет

этим может заняться система искусственного интеллекта. Благодаря этому эффективность возрастет в разы, а нагрузка для банков и потребителей снизится [4].

Применение технологии в приложениях Blockchain

Класс приложений	Области применения приложений
Blockchain 1.0	
Информация о конкретной транзакции	Системы переводов и платежей
Blockchain 2.0	
Финансовые транзакции	Акции компаний, ценные бумаги
Частные документы	Договоры, завешания, подписи, доверенности
Документы, требующие засвидетельствования	Свидетельства о собственности, страховые свидетельства
Регистрация нематериальных активов	Торговые марки, авторские права, патенты
Blockchain 3.0	
Свидетельства и лицензии, заверяемые государством	Лицензии на право занятия определенными видами деятельности
Удостоверения, заверяемые государством	Удостоверения паспорта, водительские удостоверения
Информация и документация в сфере науки и образования	Данные о научных работниках, информация об обучающихся и преподавателях
Информация и документация в сфере ЖКХ	Показатели потребления воды, электроэнергии, телекоммуникационных услуг

На базе блокчейн уже реализовано несколько проектов мирового уровня. Например, в России – пилотный проект по разработке платформы для работы Росреестра. В США и Бразилии тестируют систему, которая позволяет идентифицировать личность. Финляндия нашла применение платформе для идентификации беженцев.

Внедрение блокчейн-технологии замедляется в связи со следующими проблемами: низкая производительность в сети, недостаток специалистов в данной области, сложность хранения данных на пользовательских компьютерах, неусовершенствованное законодательство. Все эти проблемы, по мнению экспертов, будут решены через два года. Именно поэтому можно с уверенностью сказать, что технология, которая сможет перевернуть не только финансовую индустрию, но и другие сферы жизни уже существует [5].

ЛИТЕРАТУРА

1. Форк А. Bitcoin. Больше чем деньги. – М.: Мир, 2014. – 280 с.
2. Поппер Н. Цифровое Золото. Невероятная история Биткойна или о том, как идеалисты и бизнесмены изобретают деньги заново. – М.: Вильямс, 2016. – 350.
3. Свон М. Блокчейн. Схема новой экономики. – М.: Олимп-бизнес, 2017. – 240 с.
4. Петров А. Цифровые цели поставок и технологии на базе блокчейн в совместной экономике // International Journal of Open Information Technologies. – 2017. – № 8.
5. Аксенов А. Тенденции развития международных платежных систем и систем расчетов по ценным бумагам // Деньги и кредит. – 2008. – № 8.

АНАЛИЗ СПЕЦИАЛИЗИРОВАННЫХ ИАС ДЛЯ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

П.В. Прокушев, М.М. Джаналиев, студенты;

А.С. Колтайс, аспирант; Ю.А. Рубцова, студентка

*Научный руководитель Е.М. Давыдова, доцент каф. КИБЭВС, к.т.н.
г. Томск, ТУСУР, каф. БИС и КИБЭВС, pasha.prokyshev@mail.ru
Проект КИБЭВС-1703 «Методика работы с системой СПАРК»*

Любое предприятие, существующее в условиях жёсткой рыночной конкуренции рынка, особенно с учетом российских реалий, выражающихся в политических, инвестиционных, валютных, информационных, технологических и прочих средовых рисках, вынуждено заботиться о создании надежной системы экономической безопасности.

Каждый предприниматель хочет быть уверен в надёжности партнёра, обезопасить свою деятельность и минимизировать риски. Для этого ему следует задуматься о том, чтобы проверять потенциального партнёра перед заключением договора, особенно когда работает с крупными суммами.

Поэтому, проверка юридических лиц (контрагентов) является одним из главных направлений в деятельности служб безопасности. Это обусловлено, прежде всего, ужесточением российского законодательства и ответственности в части ведения дел с «фирмами-однодневками» и «обналичивающими конторами».

Для решения таких задач существуют специализированные информационно-аналитические системы, позволяющие проверить надёжность любой организации, найти компании – потенциальных клиентов, удовлетворяющих определённым критериями, отслеживать изменения деятельности своих партнёров.

Использование ИАС для проверки контрагентов. Прежде чем заключить важную сделку, многие компании предпочитают сначала убедиться, в добросовестности и законности своего партнера. Детальное изучение дела может показать плачевное состояние компании, а в отдельных случаях даже его банкротство. Исходя из этого проверка контрагента – важное дело перед заключением любой сделки.

Детальную проверку можно проводить в случаях, когда невыполнение договора может привести к большому вреду. Большинство экспертов рекомендуют, начать проверку с контроля над тем, как платит налоги контрагент. Налоговая проверка контрагента один из способов проверить компанию на платежеспособность.

Следующим шагом нужна проверка контрагента по ИНН. Стоит убедиться, что сторона, которая предлагает сделку, имеет настоящий ИНН, а не случайный набор цифр. Данный процесс не сложный, настоящий номер имеет некоторый алгоритм, в поддельном номере такой закономерности нет.

Проверка надежности контрагента поможет в дальнейшем избежать многих проблем. Поэтому нужно серьезно к этому отнестись, в этом могут помочь специализированные учреждения, в которых можно заказать услуги по проверке контрагентов. Это экономит не только время, но и много денег.

Сравнительный анализ ИАС для проверки контрагентов. На сегодняшний день в России существует около десяти систем для проверки контрагентов, наиболее известными из них являются: СПАРК [1], Прима-Информ [2], Интегрум [3], Контур.Фокус [4], Seldon.Basis [5], Глобас-і [6].

Все системы имеют сходства и различия, плюсы и минусы, но цель одна – помочь пользователю сделать оптимальный выбор, выстроить стратегию видения бизнеса на основе агрегированных и структурированных данных о ЮЛ и ИП, снабжённых индикаторами надёжности или рисков на основе анализа некоторых показателей.

На рис. 1 представлена информация о 13 различных ИАС для проверки контрагентов. Этот список не исчерпывающий, но достаточный, чтобы представить, что должна иметь система проверки контрагентов, а какие параметры являются особенными характеристиками той или иной системы, позволяющей ей проявить свою конкурентоспособность на рынке.

Все системы объединяют в себе информацию из открытых источников – государственных реестров: регистрационные данные, правовая среда, торговая деятельность. Такая база данных – обязательная часть системы. Это именно то, что позволяет пользователю системы

получить всю информацию в одном месте, а не заходить на десяток различных веб-сайтов, где представлены эти реестры.

Параметр	СПАРК	Интерум	Seldon.Basis	Прима-Информ	Контур. Фокус	UNIRATE24	Casebook	Audit-It.ru	1cont.ru	DL CONSULTING	ЛИК: ЭКСПЕРТ	РискЭксперт	ЗАЧЕСТНЫЙБИЗНЕС.РФ
Поиск в системе	+	+	+	+	+	+	+	+	+	+	+	+	+
Данные ЕГРЮЛ/ЕГРИП	+	+	+	+	+	+	+	+	+	+	+	+	+
Правовая среда													
Арбитражная практика	+	+	+	+	+	+	+	+	+	+	+	+	+
Сообщения о банкротстве	+	+	+	+	+	+	+	+	+	+	+	+	+
Исполнительные производства	+	+	+	+	+	+	+	+	+	+	+	+	+
Торговая деятельность													
Участие в государственных закупках	+	+	+	+	+	+	+		+	+	+	+	
Реестр недобросовестных поставщиков	+	+	+	+		+	+		+	+	+	+	
Финансовое состояние компании													
Бухгалтерские отчетности, фин. Показатели	+	+	+	+	+	+	+	+	+	+	+	+	+
Инструменты анализа													
Финансовый анализ	+	+	+		+		+		+	+	+	+	
Оценка благонадежности компании	+	+	+				+		+	+	+	+	
Оценка финансовой устойчивости	+	+	+				+		+	+	+	+	
Оценка кредитоспособности	+	+	+			+	+		+	+	+	+	
Визуализация связей	+	+	+				+					+	
Онлайн проверка аффилированности	+	+	+				+						
Стоимость подписки													
Безлимитный тарифный план , тыс. р. в год	от 268	от 180	99	от 10	от 22	от 18	от 48		от 19.9	нет подписки	от 44	нет подписки	
Пробная версия													
	+	+	+	+	+	+			+		+		

Рис. 1. Сравнение информационно-аналитических систем для поиска и проверки контрагентов

Важной частью ИАС для проверки контрагентов является наличие инструментов анализа. Качественно проработанные инструменты анализа, предоставляют пользователю в графическом или текстовом виде информацию, например, оценку рисков, графики изменения и анализ финансовых показателей, связи компании и т.д. Это очень удобно и экономит время пользователя. Список тех или иных инструментов анализа варьируется от системы к системе. На рисунке их представлено всего шесть, но на самом деле инструментов существует намного больше. По рис. 1 можно сказать, что ИАС СПАРК, Seldon.Basis, Casebook имеют наиболее широкий набор инструментов анализа.

На сегодняшний день в России существует более десяти ИАС для проверки контрагентов. Все системы собирают примерно одинаковую информацию о компаниях, но функционал их сильно отличается. Нельзя однозначно сказать, какая система лучше или хуже. При выбо-

ре ИАС для предприятия, нужно исходить из того, как и для каких целей будет использоваться данная система.

Заключение. Подводя итоги, можно сделать вывод, что сервисы, ориентированные на проверку контрагента, – это удобный и полезный инструмент для тех, кто серьезно относится к безопасности собственного бизнеса. При помощи подобных сервисов происходит огромная экономия времени в компании, в то же время проверка вручную из открытых источниках может занимать по несколько часов. Лидерами исходя из таблицы сравнения, можно выделить два сервиса это «СПАРК» и «Seldon.Basis», так как по функциональным возможностям, они отвечают всем требованиям, предъявляемым сотрудниками, которые проверяют контрагентов, а также в сервисах происходит постоянное обновление данных, и выполняется работа по поддержанию работоспособности сайтов.

ЛИТЕРАТУРА

1. Прима-Информ – сервис проверки контрагентов [Электронный ресурс]. – Режим доступа: <https://www.prima-inform.ru/> (дата обращения: 15.02.2018).
2. Интегрум – Информация. Работа. Деньги [Электронный ресурс]. – Режим доступа: <https://integrum.ru/> (дата обращения: 15.02.2018).
3. Контур.Фокус. Веб-сервис для быстрой проверки контрагентов [Электронный ресурс]. – Режим доступа: <https://focus.kontur.ru/> (дата обращения: 15.02.2018).
4. Проверка контрагента. Проверка ИНН, анализ рынка – СПАРК [Электронный ресурс]. – Режим доступа: <https://www.spark-interfax.ru/> (дата обращения: 19.02.2018).
- 5 Seldon.Basis – поиск и проверка контрагентов [Электронный ресурс]. – Режим доступа: <http://basisseldon.ru/> (19.02.2018).
- 6 Глобас-і. Информационно-аналитическая система [Электронный ресурс]. – Режим доступа: <https://globas.credinform.ru> (дата обращения: 25.02.2018).
- 7 Колтайс А.С. Информационно-аналитическая система «СПАРК» при обеспечении экономической безопасности предприятия // Матер. первой Всероссий. науч.-практ. онлайн-конф. «Экономическая безопасность: финансовые, правовые и IT-аспекты». – 2017. – С. 178–182.

БАНКРОТСТВО КАК ИНСТРУМЕНТ УХОДА ОТ УПЛАТЫ НАЛОГОВ

И.А. Готфрид, Е.С. Линенко, Е.Ю. Складанюк, студенты

Научный руководитель В.В. Жук, ассистент каф. КИБЭВС

г. Томск, ТУСУР, каф. КИБЭВС, naloghc@mail.ru

Проект ГПО КИБЭВС-1608 «Налоговая безопасность бизнеса»

В современном мире исследование банкротства имеет важное значение, так как количество банкротств с каждым годом увеличивается, большинство из которых имеет негативную тенденцию. Предприятия используют банкротство как попытку уклониться от налоговых и прочих обязательств.

Прежде чем переходить к рассмотрению банкротства как к инструменту ухода от уплаты налогов следует понять, что такое «банкротство». Банкротство – это результат некомпетентных действий, а также влияние различных негативных факторов как внешних, так и внутренних [1]. Процедуру банкротства следует рассматривать с двух точек зрения: экономической и юридической. С экономической точки зрения, банкротство – это результат плохого учета хозяйственных и предпринимательских рисков в деятельности организации, обусловленных прежде всего некомпетентными решениями и действиями руководства организации, то есть рисками руководителей и собственников организации. Банкротство с юридической точки зрения – это возможность положительного решения денежных вопросов организации с кредиторами. В настоящее время законодательство помогает защищать интересы как должников, так и кредиторов, давая вторым возможность вернуть вложенные средства за счет продажи имущества должника, либо путем смены руководства и собственников организации, а также путем разнообразных реорганизационных мер. В понятии банкротства существуют способы незаконного ухода от уплаты налоговых обязательств, в том числе налогов: преднамеренное и фиктивное банкротство.

Согласно ст.196 УК РФ под преднамеренным банкротством понимается «совершение руководителем или учредителем (участником) юридического лица либо гражданином, в том числе индивидуальным предпринимателем, действий (бездействия), заведомо влекущих неспособность юридического лица или гражданина, в том числе индивидуального предпринимателя, в полном объеме удовлетворить требования кредиторов по денежным обязательствам и (или) исполнить обязанность по уплате обязательных платежей, если эти действия (бездействие) причинили крупный ущерб» [2].

При совершении организацией противоправных действий, причинивших имущественный вред кредиторам, наступает административная, субсидиарная или уголовная ответственность в зависимости от величины ущерба, который он нанес. Если банкротство наступило в следствии преднамеренных действий организации – последствия являются негативными для всех сторон.

Под фиктивным банкротством согласно ст. 197 УК РФ понимается «заведомо ложное публичное объявление руководителем или учредителем юридического лица о несостоятельности данного юридического лица, а равно гражданином, в том числе индивидуальным предпринимателем, о своей несостоятельности, если это деяние причинило крупный ущерб» [2].

Обеспеченность краткосрочных обязательств должника его оборотными активами определяется как отношение величины оборотных активов, за исключением налога на добавленную стоимость по приобретенным ценностям к величине краткосрочных пассивов, за исключением доходов будущих периодов, фондов потребления и резервов предстоящих расходов и платежей.

Банкротство организации имеет как негативные, так и положительные последствия. Положительные последствия:

1. ликвидации организации и расчет с кредиторами;
2. возможность открытия нового бизнеса;
3. замена некомпетентных руководителей на профессиональных руководителей;
4. передача бизнеса организации от государства в частные руки, и наоборот.

Негативные последствия:

1. потеря кредиторами части денежных средств;
2. возможность возникновения последующих банкротств;
3. сокращение рабочих мест, возникновение социальной напряженности, и как результат – снижение платежеспособности, а, следовательно, и покупательной способности населения;
4. снижение потребительского рынка;
5. возможность криминального передела собственности организации и разворовывания имущества, в том числе организации со значительной долей государственной и муниципальной собственности.

В настоящее время организации, у которых нет перспектив расплатиться с налоговыми долгами, задолго до начала процедуры банкротства детально продумывают последовательность своих действий. Налоговые органы приводят в пример различные схемы ухода от уплаты налогов, которые называются «серые схемы». Схемы снижающие налоговую нагрузку незаконным способом уже известны налого-

вым органам и наказываются вплоть до серьёзной уголовной ответственности.

Субсидиарная ответственность наступает в ситуациях, когда владелец фирмы не в состоянии погасить долг из-за отсутствия активов и необходимого имущества. В этом случае ответственность перекладывается на список потенциальных лиц.

Инициировать процедуру привлечения к субсидиарной ответственности могут:

1. кредиторы;
2. конкурсные управляющие;
3. уполномоченные органы (в том числе налоговые);
4. представители работников должника;
5. работники и бывшие работники должника [3].

Заключение. Банкротство как способ ухода от уплаты налогов является актуальной проблемой в современном мире. На сегодняшний день установить факт преднамеренного или фиктивного банкротства достаточно сложно. Но налоговыми органами ведется создание различных приемов и способ для выявления и прекращения нелегальных схем ухода от уплаты налогов. Одним из таких стало модернизация системы субсидиарной ответственности.

ЛИТЕРАТУРА

1. Федеральный закон «О несостоятельности (банкротстве)» от 26.10.2002 № 127-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_39331/ (дата обращения: 23.02.2018).
2. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 24.02.2018).
3. Субсидиарная имущественная ответственность руководителей и учредителей должника (банкрота) [Электронный ресурс]. – Режим доступа: <https://www.auditit.ru/articles/account/court/a52/918013.html> (дата обращения 27.02.2018).

НОВЫЙ ПОДХОД К ОЦЕНКЕ ПЕРСОНАЛА В СИСТЕМЕ КАДРОВОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

А.А. Воронович, студент

*Научный руководитель С.В. Глухарева, ст. преп. каф. КИБЭВС
г. Томск, ТУСУР, nastya.voronovich@mail.ru, samantases@mail.ru*

В настоящее время оценка персонала является основной составляющей в системе управления персоналом и функционирования предприятия в целом. Оценка персонала – это «система, позволяющая из-

мерить уровень профессиональной компетенции работников, их потенциал и результаты работы» [1].

В науке выделяют традиционный и современный подходы к оценке персонала. Традиционный подход – это подход, который подразумевает оценку персонала, ориентированную на результат проделанной работы. Преимуществами традиционного подхода являются его простота, малые издержки, единообразие оценки и общедоступность, не требуется специальной подготовки, возможность сравнения работников между собой, отслеживание динамики их изменения во времени, однако здесь не учитываются личностные компетенции работника в рамках кадровой безопасности предприятия. Недостаток данного подхода – подход нацелен на конкретного работника и основывается исключительно на оценке сотрудника руководителем, ориентирован на достигнутые результаты и не учитывает долгосрочной перспективы развития организации и потенциала сотрудника.

Современный подход предполагает оценку персонала, ориентированную на развитие компании. Современный подход к оценке персонала отличается от традиционного подхода целями, широтой, методологическим аппаратом, а также использованием информационных технологий в процессе оценки для обеспечения кадровой безопасности предприятия. «Появляются новые инструменты, опирающиеся на современные технологические возможности, например, появление электронных индивидуальных деловых упражнений, или e-traits. Основное преимущество упражнений в формате e-tray состоит в том, что симуляция рабочей среды становится интерактивной, т.е. появление новых документов происходит по мере и в прямой связи с действиями участника» [2]. Постоянное развитие информационных и компьютерных технологий – это важный фактор для оценки персонала на предприятии. Процесс оценки персонала продолжается непрерывно, поэтому необходимы новые подходы к оценке персонала.

В системе кадровой безопасности предлагается новый подход к подбору персонала, который включает три составляющие: это, во-первых, сбор информации о сотруднике и ее качественный анализ, во-вторых, использование комплекса методов для достоверной оценки кандидата от анкетирования до интервью, и, наконец, определения уровня благонадежности. Новый подход позволяет составить полный портрет сотрудника. Совокупность методов можно использовать не только на этапе подбора, но и на этапе аттестации, сопровождения сотрудника. В рамках данного подхода разработана рекомендательная система, позволяющая в автоматическом режиме определять уровень благонадежности. В рамках этой системы можно получать и рекомен-

дации для дальнейшего обучения и развития сотрудника, что говорит об индивидуальном подходе в рамках развития и обучения персонала.

Таким образом, данный подход позволит повысить уровень развития персонала и уровень кадровой безопасности предприятия.

ЛИТЕРАТУРА

1. Маслова В.М. Управление персоналом. – М.: Юрайт, 2013. – 492 с.
2. Современные методы оценки персонала [Электронный ресурс]. – Режим доступа: <http://hrdocs.ru/poleznaya-informacziya/sovremennyye-metodyi-ocenki-personala/>
3. Рыжов Р.О. Кадровая безопасность: опыт социологической концептуализации [Электронный ресурс]. – Режим доступа: <http://www.ibl.ru/konf/151211/kadrovaia-bezopasnost.html>
4. Козак Н.Н. Оценка персонала и эффективности управления. – М: Издательские решения, 2016.
5. Постоева Ю.Н. Современные подходы к оценке профессиональных компетенций сотрудников организации // Инновационные технологии в образовании и науке: матер. II Междунар. науч.-практ. конф. Чебоксары, 10 сент. 2017 г. / Редкол.: О.Н. Широков и др. – Чебоксары: ЦНС «Интерактив плюс», 2017. – С. 376–381.
6. Хруцкий В.Е. Оценка персонала: современные системы и технологии. Настольная книга кадровой службы / В.Е. Хруцкий, Р.А. Толмачев. – М: Финансы и статистика, 2004. – 176 с.
7. Соломанидина Т.О. Кадровая безопасность компании: учеб. пособие / Т.О. Соломанидина, В.Г. Соломанидин. – 2-е изд., перераб. и доп. – М.: ИНФРА-М, 2017. – 559 с.

РЕЗУЛЬТАТИВНОСТЬ НАЛОГОВЫХ ПРОВЕРОК И СОВЕРШЕНСТВОВАНИЕ МЕХАНИЗМА ИХ ПРОВЕДЕНИЯ

В.Ю. Арвачёв, Д.Б. Жалсанова, студенты

Научный руководитель В.В. Жук, ассистент

г. Томск, ТУСУР, каф. КИБЭВС, naloghc@mail.ru

Проект ГПО КИБЭВС-1608 «Налоговая безопасность бизнеса»

Налоговый контроль является сложным механизмом, системой экономико-правовых мер налоговых органов, который направлен на сбор информации об исполнении налогоплательщиком своих обязательств.

В системе налогового контроля налоговые проверки подразделяются на камеральные и выездные. Налоговые проверки являются формой реализации налоговыми органами налогового контроля.

Главная цель – обнаружение и пресечение случаев нарушения налогового законодательства, проверка подлинности предоставляемых данных, легальности производимых операций, а так же привлечение к ответственности налогоплательщиков нарушивших обязанности, возложенные законом. Налоговый контроль считается наиболее важным условием функционирования налоговой системы. В условиях отсутствия или же невысокой эффективности этого инструмента, не приходится рассчитывать, что налогоплательщики станут вовремя и в полном размере уплачивать обязательные государственные платежи. Эффективность налогового контроля определяется исходя из полноты поступления налоговых доходов в бюджет Российской Федерации и затрат на осуществление такого контроля.

Несмотря на постоянное совершенствование базы нормативно-правового регулирования проведения камеральных и выездных проверок, налоговые органы, при осуществлении таких проверок, сталкиваются с проблемами как организационного, так и нормативно-правового характера, которые мешают повышению эффективности таких проверок. Правильная организация контрольной работы налоговых органов позволяет существенно увеличить поступления платежей в бюджет Российской Федерации, однако без всесторонней и правильной оценки ее результатов невозможно выявить наиболее эффективные направления налогового контроля.

В настоящее время проблема оценки эффективности налогового контроля актуальна, поскольку от этого и от качественной организации контрольной работы налоговых органов, в немалой степени зависит собираемость бюджета страны, что в свою очередь оказывает влияние на благосостояние населения.

Анализ показателей эффективности проведения налоговых проверок свидетельствует в целом об улучшении контрольной работы. Так, в 2016 г. произошло увеличение процента результативности проверок с 15 до 19%, а за восемь месяцев 2017 г. в федеральный бюджет поступило 5,8 трлн. руб., что на 32% больше соответствующего периода прошлого года. Поступления в консолидированный бюджет Российской Федерации выросли на 19% и составили 11,2 трлн. руб., прослеживается весьма положительная тенденция в увеличении суммы доначислений. Особое внимание уделено выполнению задачи по качественному администрированию страховых взносов. За январь-август 2017 г. поступления страховых взносов в государственные внебюджетные фонды составили 3,6 трлн рублей, что на 8%, или на 272 млрд. руб., больше соответствующего периода прошлого года и превышает темп роста заработной платы. По итогам первого полуго-

дия 2017 г. количество выездных проверок снижено еще на 22%, а их результативность выросла в 1,4 раза. В бюджет Российской Федерации по результатам контрольно-аналитической работы с начала года поступило 131 млрд. руб., что на 7% больше аналогичного периода прошлого года. Высокие результаты контрольной работы, во многом достигнутые за счет качественного межведомственного взаимодействия с федеральной таможенной службой России принесло пресечение непрозрачных схем поставок электротехники, фармацевтической продукции и автокомпонентов за первое полугодие принесло в бюджет Российской Федерации более 40 млрд. руб. Были расширены полномочия налоговых органов – появились новые инструменты противодействия уклонению от уплаты налогов что повысило эффективность проведения налоговых проверок. Одним из инструментов оценки благонадежности контрагентов является Единый государственный реестр юридических лиц. В 2017 г. из него исключено 20% фирм с признаками фиктивности. Всего в реестр внесено более 250 тысяч записей о недостоверности сведений [1].

Изменения в налоговых проверках на 2018 г. направлены на уменьшение общего числа проверок. В 2018 г. срок проведения камеральных проверок сократится до одного месяца. Сейчас этот срок составляет 3 месяца. Налоговики часто проводят так называемые дополнительные мероприятия налогового контроля. С 2018 г. по итогам дополнительных мероприятий налоговые инспекторы будут составлять отдельный акт, в котором они должны указать суть мероприятий и свои выводы. У компаний будет право ознакомиться с актом и подать возражения. Если компания сдаст уточненную декларацию, в которой уменьшен налог, при повторной выездной проверке проверять будут только обоснованность уменьшения [2].

По поручению президента до конца года Генеральная прокуратура Российской Федерации и Правительство Российской Федерации должны подготовить проект, который ограничит число внеплановых неналоговых проверок. Кроме того, чиновники должны будут сократить срок внеплановых проверок до 10 рабочих дней [2].

Для доказательства вины налогоплательщика необходимо подтвердить, что он осознавал противоправность совершаемых действий и ожидал конкретных последствий. При этом в актах фискальных проверок недостаточно перечислить операции, которые фискальные службы считают недобросовестными или противоправными – по каждому пункту должно быть прописано конкретное действие плательщика налогов (или подчиненных ему лиц), которое привело к правонарушению, а также конкретное последствие для бюджета Российской Федерации [2].

На основании вышеизложенного подведем итог, что Федеральная налоговая служба Российской Федерации увеличила результативность своей деятельности. Были уменьшены количество выездных проверок и также сократился срок проведения камеральных проверок до одного месяца, увеличена собираемость налогов в бюджет страны, за счет повышения эффективности, улучшения контрольной работы, а также качественного межведомственного взаимодействия с Федеральной таможенной службой Российской Федерации.

ЛИТЕРАТУРА

1. ЦЕНТРИНФОРМ. Итоги проверок работы ФНС каждому за 2017 г. [Электронный ресурс]. – Режим ресечение доступа: https://7405405.ru/news/podvedeny_itogi_raboty_fns_za_vosem_mesyatsev_2017_goda/ (дата обращения: 24.02.2018).

2. Бухгалтерия.ру «Налоговые проверки в 2018 году [Электронный ресурс]. – Режим доступа: <http://www.buhgalteria.ru/article/n160575/> (дата обращения: 25.02.2018).

СЕКЦИЯ 6

ЭКОЛОГИЯ И МОНИТОРИНГ ОКРУЖАЮЩЕЙ СРЕДЫ. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

СЕКЦИЯ 6

ЭКОЛОГИЯ И МОНИТОРИНГ ОКРУЖАЮЩЕЙ СРЕДЫ. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

*Председатель секции – Карташев А.Г., проф. каф. РЭТЭМ, д.б.н.;
зам. председателя – Денисова Т.В., доцент каф. РЭТЭМ, к.б.н.*

ВЛИЯНИЕ СЕНОМАНСКИХ РАСТВОРОВ НА РАЗВИТИЕ МОЛЛЮСКОВ

А.А. Данцова, студент; А.П. Шкарупо, аспирант

Научный руководитель А.Г. Карташев, д.б.н., проф. каф. РЭТЭМ

Развитие нефтедобычи в Западной Сибири привело к изменениям. Нарушение естественной среды обитания начинается с проведения разведочных работ. Разливы сеноманских растворов при нефтедобыче оказывают негативное влияние на экосистемы. Техногенные аварии с разливом высокоминерализованных сеноманских растворов на поверхности могут оказывать негативное влияние на водные экосистемы. По динамике размножения, изменений численности особей, поведенческих реакциях моллюсков можно судить об изменениях в водной среде [1].

Для экспериментального исследования были выбраны моллюски вида физа. Моллюск Физа Относится к классу моллюсков, отряд лёгочные моллюски, подотряд сидячеглазые, семейство физиды. Представители этого семейства обладают раковинами, завитыми в левую сторону [2]. Моллюски Физа небольшого размера, в неволе достигает 1,5–2 см в длину. Обладает хрупкой раковиной, закрученной в левую сторону, в отличие от других видов улиток. От других видов отличается способностью выделять клейкую нить, соединяя дно водоёма и поверхность воды. По этой нитке физа легко скользит вверх и вниз, чтобы глотать воздух с поверхности [3]. Физы живут не долго, по сравнению с другими видами. Улитку физи можно найти в Азии, северных краях Африки и Европе. Главное условие – тёплый климат и медленно текущая или стоячая вода: реки, озёра и пруды [4]. Не прихотливы к корму, легко питаются животными отходами и водорослями. Разбавить рацион можно мелко порубленной зеленью или овощами.

Целью данной работы является исследование влияния сеноманских растворов на развитие моллюсков. Объектом исследования являются моллюски физы, при действии растворов минерализованных сеноманских вод в разных концентрациях.

Исследование проведено на двух экспериментальных группах с параллельным контролем, группой без внесения загрязнителя. Одна группа помещалась в среду с концентрацией 200 мл/л, вторая с концентрацией 50 мл/л. Время наблюдений составило 10 дней.

В первые сутки опытов в концентрации 200 мл/л погиб один моллюск. В дальнейшем погибшие моллюски в концентрации сеноманских растворов 200 мл/л обнаружены на вторые, шестые, седьмые и восьмые сутки. На девятые сутки исследований в концентрации 200 мл/л погибли все моллюски. У моллюсков было обнаружено высыхание мягких тканей.

В концентрации 50 мл/л погибших моллюсков и изменений в их внешнем виде не выявлено.

В результате полученных данных был построен график выживаемости моллюсков (рис. 1).

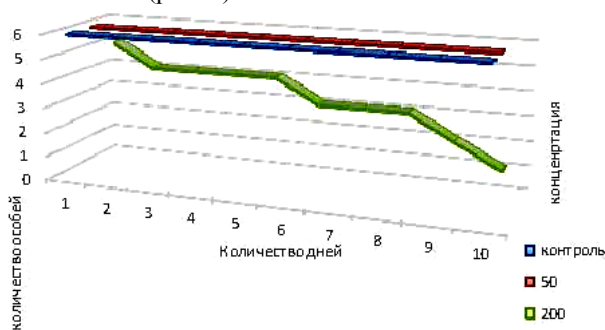


Рис. 1. Выживаемость моллюсков

Анализируя данные, представленные на графике, можно отметить наступление смерти на первые сутки при концентрации 200мл/л и большое количество умерших на девятый день. В концентрации 50мл/л наглядных изменений не было обнаружено.

На основании проведенных исследований по влиянию сеноманских растворов на пресноводных моллюсков можно сделать следующие выводы:

1. Показано, что при загрязнении среды обитания моллюсков сеноманскими растворами снижается выживаемость в концентрации 200 мл/л.

2. Моллюски вида физы устойчивы к загрязнениям с небольшой концентрацией токсина в их среде обитания.

ЛИТЕРАТУРА

1. Карташев А.Г. Адаптация животных к хроническим факторам // LAP LAMBERT Academic Publishing: Saarbrücken, 2014. – 260 с.
2. Кулюкина Е.В, Карташев А.Г. Влияние сеноманских вод на сообщества раковинных амёб // Вестник НВГУ. – 2017. – № 1.
3. Физа: самый распространенный вид аквариумных улиток, секреты содержания. [Электронный ресурс]. – Режим доступа: <http://mirpodsteklom.ru/zhivnost/fiza.html#i-7> (дата обращения: 28.02.2018).
4. Спорные улитки – физы [Электронный ресурс]. – Режим доступа: <http://nashirybki.ru/bespozvonochnye/ulitka-fiza.html> (дата обращения: 28.02.2018).

ЭКОЛОГИЧЕСКИЕ ПОКАЗАТЕЛИ РЫБ ОЗЕРА ИССЫК-КУЛЬ

А.А. Гайворонских, студент

*Научный руководитель А.Г. Карташев, проф. каф. РЭТЭМ, д.б.н.
г. Томск, ТУСУР, kartag@rambler.ru*

Промысловые уловы рыб на озере Иссык-Куль за период 1995–2008 года представлены в таблице. После 2003 г. введены ограничения и запреты на местном уровне и в последующем на государственном на запрет вылова определенных видов рыб. Но положительных результатов это не дало.

**Промысловые уловы рыб на озере Иссык-Куль за 1995–2008 года,
данные представлены в центнерах**

Виды рыб	Чебак	Чебачек	Сиг	Судак	Форель	Лещ	Всего
1995	261±10	900±20	87±6	66±5	46±4,5	102±6,7	1465,5
1996	68±5	260±10	70±5	34±4	61±5	82±6	575
1997	81±6	249±10	49±4,5	21±3	35±4	62±5	497
1998	80±6	93±6	50±4,5	2±0,6	2±0,6	70±5	297
1999	37±4	36±4	29±3,7	3±1	2±0,6	52±3,7	159
2000	42±4	6±1,5	28±3,6	1±0,5	0,5±0,5	28±4,7	105,5
2001	86±6	2±0,8	10±2	3±0,6	0,6±0,5	18±3	119,6
2002	39±4	8±1,8	6±1,5	1±0,5	1,7±1	2±0,9	57,7
2003	10±2	32±3,7	4±1,2	5±1	2,6±0,9	–	53,6
2004	8±1,8	5±1	18±3	4±1	2±0,6	–	37
2005	8±1,8	–	11±2	–	2,8±0,9	–	21,8
2006	6±1,5	–	6±1,5	–	2,5±0,8	–	14,5
2007	6±1,5	–	5±1	–	2±0,6	–	13
2008	5±1	–	10±2	–	2±0,6	–	17
Всего	734	1591	383	140	162,7	416	3414

В августе 2008 г. введен мораторий озере Иссык-Куль на вылов рыбы, на пять лет. Исключением являлась вылов рыбы для научных целей, воспроизводства рыбы и любительское рыболовство. Меры введены для увеличения рыбных запасов озера Иссык-Куль. До введения моратория насчитывалась 700 т рыбы, после пяти лет моратория количество рыбы должно было увеличиться до 3500 т но результаты не улучшились. Браконьеры как занимались промыслом до моратория, так и занимались и во время моратория. Самарбек Кучуков сказал, что было недостаточное финансирование для регулирования озера [1].

Чебак распространен по всему озеру равномерно, но выловы приходится в основном в городе Балыкчы, и в городе Каракол, в селах на южной стороне Улахол, Ак-терек, Покровка, на северной стороне Григорьевка, Ананьево, Кутурга, восточной стороне в селе Тюп. На эти участки приходится 80% вылова чебака, в остальных селах не более 20% уловов. Иссык-Кульский чебачек обитает по всему побережью озера, выловы чебачка приходилось в основном в нерест. Более 60% уловов приходится на села Кутурга, Тюп, Григорьевка, Тамчы, Черепыкты, Улахол, 30% на города Каракол и Балыкчы, и 10% на все остальные рыболовные участки. Рыбаки используют мелкочейные сети.

Форель распространена неравномерно, в основном места впадения реки и каменистое дно с большой глубиной. Уловы форели приходится, когда рыба идет на нерест. Более 68% уловов приходится, на южном и восточном побережье в селах Покровка, Барскоон, Томга, Тосор, Каджи, Бокомбаево, Ак-терек, Тюп, Кутурга и город Каракол. Остальные 32% уловы приходится на северном и западном побережье. Устанавливаются крупночейные сети, неводы и бредни.

Сиг обитает по всему озеру. Вылов сига проходит круглый год. В теплое время рыбаки ставят сети до глубины 50 метров, зимой сиг уходит на глубоководные участки более 150 метров. Самые большие уловы сига в городе Балыкчи более 30% от всех рыболовных участков. Остальные 70% приходится на все остальные рыболовные участки озера.

Судак обитает по всей акватории озера. Передвижение судака зависит от передвижения молоди, которая служит пищей судаку. Большие уловы судака 74% в селах Ананьево, Тюп, Григорьевка, Кутурга, Чырпыкты, Тамчы, Покровка, Бокомбаево, Ак-терек, и в городах Каракол и Балыкчы. Рыбаками устанавливаются крупночейные сети, в заливах используют бредни.

Лещ распространен неравномерно, вылов леща приходится на 80% на восточном побережье в селе Тюп, Покровка и город Каракол,

на западном побережье город Балыкчи и село Улахол. Таким образом, неконтролируемый вылов промысловой рыбы оз. Иссык –Куль приводит к истощению рыбных запасов и нуждается в искусственном зарыблении озера.

ЛИТЕРАТУРА

1. Информационное агентство Кыргызстана [Электронный ресурс]. – Режим доступа: <http://u.to/pFJWEQ>
2. Кыргызская Республика, архив Иссык-Кульской области. Промысловые уловы рыб 1995–2017.

ОЦЕНКА ИЗМЕНЕНИЙ БОЛОТНЫХ ЛАНДШАФТОВ ЗАПОВЕДНИКА «ВАСЮГАНСКИЙ» В ПРЕДЕЛАХ ТОМСКОЙ ОБЛАСТИ В ПЕРИОД С 1984 ПО 2016 ГОДЫ

В.И. Иванов, студент

Научный руководитель Л.Г. Колесниченко, с.н.с. НИИ ББ ТГУ

Т.В. Денисова, доцент кафедры РЭТЭМ

г. Томск, ТУСУР, каф. РЭТЭМ, ehome.qq@gmail.com

Болота Западной Сибири играют ведущую роль в динамике регионального и глобального биогеохимического цикла углерода, так как здесь сосредоточена значительная часть его мировых запасов [1, 2, 3]. Согласно некоторым оценкам, вклад болот России в эмиссию метана может составлять от 25 до 50% от общего потока, причем половина приходится на долю западносибирских болот [3]. Трансформация болот, вызываемая их хозяйственным освоением и изменениями климата, отражается в разбалансированности биогеохимических потоков, поэтому изучение функционирования болотных экосистем Западной Сибири является в настоящее время чрезвычайно актуальной задачей.

Вопросам заболачивания Сибири посвящено большое количество работ [4–8], однако недавно предоставленная возможность в системе Google Earth Pro свободного использования разновременных космических снимков, помогает перейти на новый уровень понимания масштабов проблемы.

Целью нашего исследования является анализ изменения болотных ландшафтов территории заповедника «Васюганский» в пределах Томской области за тридцатилетний период.

Как известно, на территории Томской и Новосибирской областей находится один из крупнейших болотных массивов мира – Большое Васюганское Болото (БВБ) [9]. В 2006 г. эта территория приобрела

статус заказника [10], поэтому с уверенностью можно утверждать, что антропогенное воздействие на нее, по крайней мере, в течение 12 лет было минимально и все изменения, происходящие здесь в настоящее время, носят исключительно природный характер.

При исследовании динамики ландшафтов нами было проведено дешифрирование синтезированных космических снимков Landsat за 1984 и 2016 гг. (Google Earth Pro) с использованием стандартных средств геоинформационной системы ArcGIS 10.0.

Результаты дешифрирования разновременных снимков БББ в пределах Томской области представлены на рис. 1. В ходе работ мы выявили изменения границ и ландшафтной структуры исследуемой территории, произошедшие за тридцать лет под влиянием природных факторов.

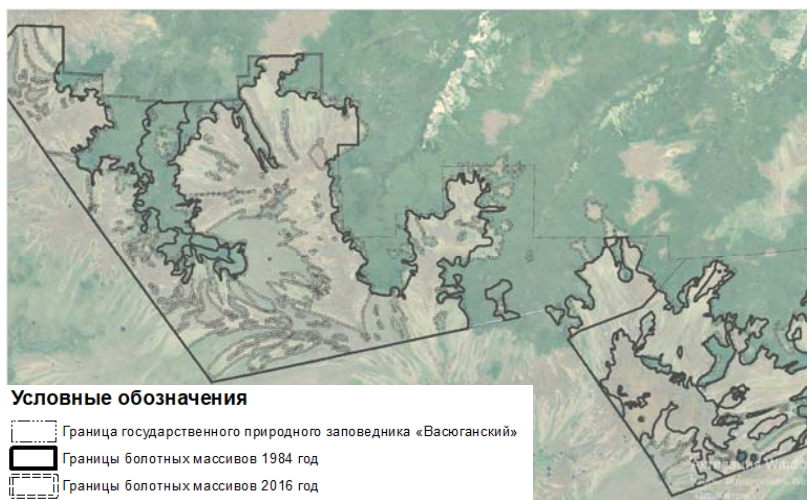


Рис. 1. Границы болотных массивов в 1984 и 2016 гг. (Google Earth Pro)

Были установлены как участки, подвергнутые интенсивному заболачиванию, так и участки, зарастающие лесом. Такое сочетание процессов заболачивания и залесения и ранее было отмечено для зоны южной тайги Западной Сибири [8]. Так как в этой зоне развитие болот происходит под воздействием подземных и атмосферных вод (аллохотное заболачивание), то основной причиной изменений границ болотных ландшафтов, по-видимому, является изменчивость гидроклиматических условий, которая приводит к изменению интенсивности дренирования территории [8]. Слабая степень дренированности уси-

ливаает процесс заболачивания, а ее увеличение ведет к залесению участков [7].

Таким образом, обработка разновременных космических снимков Landsat и формирование цифровых слоев в ArcGIS позволили показать изменение пространственной структуры БББ за тридцатилетний период.

В дальнейшем необходимо проведение комплексных междисциплинарных исследований компонентов ландшафтов территорий, претерпевших изменения за столь незначительное время, в сравнении их с неизменными аналогами, что будет шагом к моделированию функционирования болотных массивов.

ЛИТЕРАТУРА

1. Пьявченко Н.И. Торфяные болота, их природное и хозяйственное значение. – М.: Наука, 1985. – 152 с.
2. Kirpotin S., Dupre B., Pokrovsky O. et al. Western-Siberian peatlands as indicator and regulator of climatic changes // IOP Conf. Series: Earth and Environmental Science 6, 2009.
3. Глаголев М.В., Сирин А.А., Лапшина Е.Д., Филипов И.В. Изучение потоков углеродсодержащих парниковых газов в болотных экосистемах Западной Сибири / Вестник ТГПУ, 2010. – 93 с.
4. Вендров С.Л., Герасимов И.П., Куницын Л.Ф., Нейштадт М.И. Влагооборот на равнинах Западной Сибири, его роль в формировании природы и пути преобразования // Известия АН СССР. Сер. геогр. – 1966. – № 5. С. 3–18.
5. Нейштадт М.И. Взаимоотношение леса и торфяного болота в голоцене (на примере Западной Сибири) // Болота и болотные ягодники: труды Дарвинского гос. заповедника. – 1979. – Вып. 15. – С. 33–45.
6. Глебов Ф.З. Взаимоотношения леса и болота в таежной зоне. – Новосибирск: Наука, 1988. – 184 с.
7. Малик Л.К. О будущем болотных массивов и возможностях восстановления северных лесов // Метеорология и гидрология. – 1992. – № 6. – С. 95–100.
8. Инишева Л.И., Березина Н.А. Возникновение и развитие процесса заболачивания на Западно-Сибирской равнине / Вестник Томского государственного университета. – 2013. – № 366. – С. 172–179.
9. Васюганское болото (природные условия, структура и функционирование) / Под ред. Л.И. Инишевой. – Томск: ЦНТИ, 2000. – 136 с.
10. Постановление администрации Томской области от 10.03.2006 №28а «О создании государственного комплексного (ландшафтного) заказника областного значения «Васюганский».

ПОЛОЖИТЕЛЬНАЯ ОЦЕНКА СИСТЕМЫ ОХРАНЫ ТРУДА ПРЕДПРИЯТИЯ И ЕЕ АНАЛИЗ

Т.А. Безъязыкова, К.В. Камянецкая, студентки

Научный руководитель С.А. Полякова, доцент каф. РЭТЭМ, к.б.н.

г. Томск, ТУСУР, каф. РЭТЭМ, bezuzykova98@mail.ru

*«Проект ГПО РЭТЭМ-1806 «Анализ охраны труда на предприятиях
Томской области»*

В современном мире системе охраны труда уделяется достаточно большое внимание. Это связано с интенсивным развитием производственной сферы и появлением новых видов деятельности.

Соблюдение ее принципов позволяет решить целый ряд задач, среди которых:

- гарантированная защита сотрудников от вредных и опасных факторов, влияющих на их здоровье или здоровье их потомства;
- снижение расходов на обеспечение производственного процесса;
- исключение серьезных экономических убытков из-за потери рабочего времени;
- исключение претензий и финансовых санкций контролирующих органов, призванных следить за соблюдением требований трудового законодательства;
- повышение производительности и качества труда персонала.

Известно, что самой высокой ценностью всегда является человек, его жизнь и здоровье. Ни размер заработной платы, ни уровень рентабельности предприятия, ни ценность производимого продукта не могут служить основанием для пренебрежения правилами безопасности и оправданием существующих угроз жизни или здоровью работников. Кроме того, в данном случае речь также идет о ценности конкретного человека как работника с присущими ему знаниями, навыками и опытом. Правильно организованная работа по обеспечению безопасности труда повышает дисциплинированность работников, что, в свою очередь, ведет к повышению производительности труда, снижению количества несчастных случаев, то есть повышает в конечном итоге эффективность работы.

Охрана труда подразумевает не только обеспечение безопасности работников во время исполнения ими служебных обязанностей. На самом деле сюда, также относятся самые разные мероприятия: например, профилактика профессиональных заболеваний, организация полноценного отдыха и питания работников во время рабочих перерывов, обеспечение их необходимой спецодеждой и гигиеническими средствами, а также выполнение социальных льгот и гарантий. Правильный

подход к организации охраны труда на рабочем месте, грамотное использование различных нематериальных способов стимулирования работников дают последним необходимое чувство надежности, стабильности и заинтересованности руководства в своих сотрудниках. Таким образом, благодаря налаженной работе системы охраны труда снижается текучесть кадров, что тоже благотворно влияет на стабильность работы всего предприятия [1].

Охрана труда сегодня, как никогда, актуальна. Трудно представить себе успешное предприятие на рынке, руководство которого халатно относилось бы к вопросам охраны труда. Прежде всего это обусловлено тем, что качественно функционирующая система охраны труда дает работникам организации уверенность в работодателе, что обеспечивает уменьшение текучки кадрового состава. Помимо этого в нашей стране законодательно предусмотрена система стимулирования того работодателя, чьи рабочие места соответствуют требованиям безопасности труда. Так например, Фонд социального страхования Российской Федерации обеспечивает финансирование некоторой части затрат предприятия, направленных на повышение уровня безопасности труда. Но также необходимо отметить, что помимо «положительно» выраженного стимула присутствует и «отрицательный», что выражено в системе административной, а порой даже уголовной ответственности для работодателя, на рабочих местах которого творится беспорядок с точки зрения охраны труда.

Вышеизложенные факторы обуславливают рост значимости безопасности жизни и здоровья трудящихся на предприятии, что приводит к развитию следующих процессов на предприятии:

- повышение комфортности и безопасности условий труда как одного из основных факторов, влияющих на производительность труда, здоровье работников;
- повышение эффективности мероприятий по улучшению условий труда, что является экономическим выражением социального значения охраны труда, как источник финансирования системы охраны труда и повышения эффективности производства.

Социальное значение охраны труда заключается в содействии росту эффективности общественного производства путем непрерывного совершенствования и улучшения условий труда, повышения его безопасности, снижения производственного травматизма и заболеваемости.

Рост производительности труда в результате увеличения фонда рабочего времени за счет сокращения внутрисменных простоев путем предупреждения преждевременного утомления, снижения числа мик-

ротравм, уменьшения целодневных потерь рабочего времени по причинам временной нетрудоспособности из-за травматизма, профессиональной и общей заболеваемости [2].

Из всего вышеизложенного можно сделать вывод, что качественно построенное функционирование системы охраны труда положительно сказывается на:

1. Финансовом благополучии предприятия за счет повышения объемов производства.
2. Создании комфортной для работников производственной среды, за счет благоприятной социальной политики в области безопасности труда.
3. Снижении общего уровня заболеваемости и профпатологии.
4. Стимулировании социального настроения среди работников.

ЛИТЕРАТУРА

1. Безопасность жизнедеятельности: учеб. пособие. – Ч. 2 / под ред. Е.А. Резчикова, В.Б. Носова. – 2-е изд., испр. и доп. – М.: МГИУ, 1999. – 248 с.
2. Трудовой кодекс Российской Федерации. – М.: Юрайт-М, 2002.

ОБЗОР ЛАБОРАТОРНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ С ЦЕЛЮ ВЫЯВЛЕНИЯ КОНКУРЕНТНЫХ ПРЕИМУЩЕСТВ ХИМИЧЕСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Е.В. Кандычева, магистрант

*Научный руководитель П.Н. Дробот доцент каф. УИ
г. Томск, ТУСУР, каф. УИ, kandycheva@mail.ru*

Лабораторные информационные системы (далее ЛИС) набирают популярность и уже давно закрепили за собой свой собственный рынок.

Химическая информационная система (далее ХИС) относится к информационным программам по надзору прекурсоров. Проведя анализ ЛИС с помощью единого реестра российских программ для электронных вычислительных машин и баз данных и списка тендеров России и Москвы на их официальных сайтах [1, 2]. Был сформирован список ЛИС включающих в себя данные в сфере по надзору прекурсоров. Проведено их анкетирование через рассылку, с целью выявления конкурентных преимуществ для формирования ценностного предложения ХИС. Данные по анкетированию представлены в таблице.

ЛИС «АЛИСА»

Краткое описание: поддерживает автоматизацию всех клинико-диагностических исследований, представленных в современной лабо-

раторной диагностике: биохимические, иммунологические, гематологические и иммуногематологические, общеклинические, гормональные, серологические, микробиологические, цитологические и гистологические, ДНК-исследования и т.д. [3].

Заключение. Программа производит учет реагентов через создания электронных журналов, так же производит расчеты и составлять отчетную документацию. Не содержит энциклопедических данных по прекурсoram.

Опрос организаций для выявления уникальных преимуществ

Организации	Работает без интер-нета?	Есть информаци-онная составляющая о веществах?	Имеется переход к Федеральным Законам?	Воз-можность составления отчета?
1	–	–	+	+
2	–	–	–	+
3	+	–	–	+
4	–	–	–	+
5	–	–	+	+

ЛИС «АРИАДНА»

Краткое описание: представляет собой набор простых в использовании модулей, которые подбираются и настраиваются для решения конкретных задач заказчика оптимальным образом [4].

Заключение. Программа формирует статистические отчеты о работе лаборатории, производит учет реагентов. Не содержит энциклопедических данных по прекурсoram.

ЛИС «АЛТЭЙ»

Краткое описание: поддерживает полный технологический цикл лаборатории от регистрации заказов до выдачи результатов и получения лабораторных журналов и статистических отчетов. Обеспечивает долговременное хранение лабораторной информации и предоставляет пользователю возможность быстрого поиска требуемых сведений в лабораторном архиве [5].

Заключение. Программа проводит расчетные процедуры, ведет электронные журналы, обеспечивает хранение данных. Не содержит энциклопедических данных по прекурсoram.

ЛИС «qMS»

Краткое описание: Автоматизация лабораторных процессов, оптимизация логистики биологического материала и контроль на всех этапах исследования [6].

Заключение. Программа направлена на лабораторные исследования, является расчетной с функцией формирования отчетов.

ЛИС «Колибри»

Краткое описание: ЛИС позволяет автоматизировать все внутренние процессы лаборатории, связанные с расчётами и документооборотом, а так же объединить процессы лаборатории с процессами прочих существующих корпоративных систем предприятия. При этом ЛИС:ЛИС может выступать как поставщиком так и потребителем данных: готовых отчетных документов или информации из базы данных [7].

Заключение. Программа ведет учет и формирует отчетную документацию включая и прекурсоры.

На основе данного анализа ЛИС были выявлены следующие основные конкурентные преимущества для ХИС:

- выполнение требований Федерального закона от 08.01.1998 n 3-фз (ред. от 03.07.2016) «о наркотических средствах и психотропных веществах» (с изм. и доп., вступ. в силу с 01.01.2017);
- идентификация веществ по их тривиальным названиям;
- экономии средств на обучении и переподготовки сотрудников в данной сфере;
- доступная информация на складах без интернета и энциклопедий;
- компактность, энциклопедии и федеральных законов(все в одном месте).

В ЛИС-ах в основном преобладают два вида: программы учета и программы анализаторы лабораторных исследований. Из исследуемых программных продуктов лишь одна содержит информационную составляющую, но не по прекурсарам.

ЛИТЕРАТУРА

1. Единый реестр российских программ для электронных вычислительных машин и баз данных [Электронный ресурс]. – Режим доступа: <https://reestr.minsvyaz.ru/reestr/> (дата обращения: 10.01.2018).
2. Список тендеров России и Москвы [Электронный ресурс]. – Режим доступа: <http://www.trade.su/> (дата обращения: 10.01.2018).
3. ЛИС «АЛИСА» [Электронный ресурс]. – Режим доступа: <http://www.galen.ru/ru/item/sendvalues/5/> (дата обращения: 15.01.2018).
4. ЛИС «АРИАДНА» [Электронный ресурс]. – Режим доступа: <http://www.bregis.ru/products/ariadna/> (дата обращения: 20.01.2018).
5. ЛИС «АЛТЭЙ» [Электронный ресурс]. – Режим доступа: <http://www.altey.ru/index.php/products/analyseru.html> (дата обращения: 10.11.2017).
6. ЛИС «qMS» [Электронный ресурс]. – Режим доступа: <https://sparm.com/products/qms/lis> (дата обращения: 10.02.2018).
7. ЛИС «Колибри» [Электронный ресурс]. – Режим доступа: <http://www.fc-c.ru/1clis/> (дата обращения: 10.02.2018).

РОЛЬ ИЗУЧЕНИЯ МЕР ПОЖАРНОЙ БЕЗОПАСНОСТИ В ПРОЦЕССЕ ПРОФЕССИОНАЛЬНОГО СТАНОВЛЕНИЯ СТУДЕНТОВ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

А.С. Канисеев, Н.С. Симкина, студенты

Научный руководитель Н.Н. Несмелова, доцент каф. РЭТЭМ, к.б.н.

г. Томск, ТУСУР, каф. РЭТЭМ, kaniseev-artyom@yandex.ru

В условиях современного общества обеспечению безопасности в различных её проявлениях уделяется достаточно большое внимание. Так, например, разрабатываются всё более надёжные способы защиты информации, системы обеспечения безопасности дорожного движения, пожарной безопасности и другие.

Прежде всего, это обусловлено развитием различных областей науки и техники, внедрением в процесс жизнедеятельности человека всё более наукоёмких «помощников». Этот процесс не обошёл стороной и профессиональную деятельность человека, и чем выше уровень научно-технического прогресса, тем выше требования по обеспечению безопасности, предъявляемые к работнику.

Пожарная безопасность – это тот вид безопасности, с которым придётся столкнуться каждому работнику или работодателю в процессе исполнения своего должностного функционала. И если в условиях производства процесс обучения мерам безопасности организован на достаточно высоком уровне через инструктирование и сдачу пожарно-технического минимума, то с получением знаний в области пожарной безопасности на этапе освоения той или иной специальности, во время обучения в высшем учебном заведении, дела обстоят не столь хорошо.

Современное образование ориентировано на компетентностный подход, при этом формируемые в процессе обучения компетенции должны в результате приводить к появлению на выходе из ВУЗа компетентного профессионала, готового к самостоятельной трудовой деятельности. Обязательной дисциплиной основных профессиональных образовательных программ (ОПОП) является дисциплина «Безопасность жизнедеятельности», которая, как правило, связана с компетенцией «готовность пользоваться основными методами защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий». Соответственно, основное содержание дисциплины отражает тематику безопасности в чрезвычайных ситуациях [1].

При этом обучению мерам пожарной безопасности в рамках курса «Безопасность жизнедеятельности» внимание практически не уде-

ляется или не уделяется совсем в зависимости от специальности, преподавателя и других аспектов. Стоит отметить, что при выполнении студентами определённых видов образовательных заданий (например, лабораторных работ) проводится инструктирование вышеупомянутых, но на деле оно, как правило, носит достаточно формальный характер.

В рамках проекта ГПО РЭТЭМ-1407 «Безопасность образовательной среды» для обучения студентов нормам и правилам пожарной безопасности была разработана образовательная программа, которая состоит из теоретического и практического модулей [2].

Данная образовательная программа включает в себя пять разделов теоретического материала и банк вопросов, из которых формируется практическая часть – тестовые задания. На данный момент предусмотрено проведение двух тестирований: первичного и итогового. Первичное тестирование направлено на оценку уровня знаний студентов в области пожарной безопасности до изучения теоретического материала, а итоговое позволяет оценить изменение этого уровня в результате обучения. При этом подбор вопросов из банка заданий осуществляется случайным образом, что позволяет избежать повторов и сделать каждое тестирование уникальным.

По результатам апробации образовательной программы с участием студентов нескольких учебных групп отмечено повышение уровня знаний участников после обучения в среднем на $1 \pm 0,22$ относительно начального уровня. Уровень знаний оценивался по количеству верных ответов на десять случайно выбранных вопросов из банка заданий. Отличие между результатами первого и второго тестирования оказалось достоверным ($p < 0,05$, критерий Манна–Уитни), следовательно – обучение с использованием разработанного электронного курса является эффективным.

Следующим шагом стало проведение тестирования преподавателей ТУСУР. Результаты показали, что средний балл по первичному тестированию у преподавателей составил 8,28, что оказалось выше, чем тот же показатель у студентов – 7,2.

Данные различия обусловлены тем, что преподаватели являются работниками высшего учебного заведения. Поэтому, согласно законодательству, они должны проходить инструктажи по пожарной безопасности и обучение пожарно-техническому минимуму с определённой периодичностью. Кроме того, знание мер пожарной безопасности является одной из профессиональных компетенций преподавателя, поскольку он несёт ответственность за безопасность студентов в учебное время. Организация эвакуации во время пожара также явля-

ется одной из обязанностей преподавателя. В то же время, среди преподавателей также выявлена группа лиц, уровень знаний которых оказался недостаточным.

В связи с этим планируется доработать образовательную программу и предложить руководству вуза использовать её для обучения профессорско-преподавательского состава. Кроме того, данная программа может быть использована в качестве альтернативы проведения противопожарных инструктажей у студентов, поскольку им также придется столкнуться с данным аспектом жизни в будущем при приеме на работу и выполнении профессиональных обязанностей.

ЛИТЕРАТУРА

1. Несмелова Н.Н., Канисеев А.С. Изучение мер пожарной безопасности как часть профессионального становления студента // Сб. науч. трудов по матер. XXVI междунар. науч.-практ. конф. «Перспективы развития науки и образования», 28 февраля 2018 г. – М.: ИП Туголуков А.В., 2018. – 52–55 с.

2. Канисеев А.С., Несмелова Н.Н. Разработка и апробация электронного курса «Пожарная безопасность в образовательной среде» // Сб. науч. трудов IV Междунар. науч. конф. «Информационные технологии в науке, управлении, социальной сфере и медицине», Томск, 5–8 декабря 2017 г.: в 2-х ч. – Ч. 2. – Томск: Изд-во НИТПУ, 2018. – С. 36–38.

ВЛИЯНИЕ НЕФТЕЗАГРЯЗНЕНИЙ НА СООБЩЕСТВА ПОЧВЕННЫХ НЕМАТОД В ЕСТЕСТВЕННЫХ УСЛОВИЯХ

Д.А. Ключева, студентка; С.А. Калашикова, ассистент

Научный руководитель А.Г. Карташев, проф. каф. РЭТЭМ, д.б.н.

Томск, ТУСУР, каф. РЭТЭМ, klyuyeva.diana@mail.ru

Действие различных фракций нефти на живые организмы различно. Легкие фракции нефти и нефтепродуктов, богатые бензином, обладают повышенной токсичностью для живых организмов. Летучие фракции проявляют эффект сразу после контакта с почвой и ее обитателями [1–4]. Для оценки состояния среды и мониторинга любых антропогенных изменений важнейшей задачей становится выявление видов-индикаторов. Эврибионтность нематод позволяет рассматривать данную группу в качестве удобного биологического теста. Популяции нематод в силу консервативных репродуктивных стратегий довольно стабильны, поэтому изменения видовой структуры и численности отдельных систематических групп объясняются нарушениями в среде их обитания [2].

Для исследования влияния нефтепродуктов на сообщество почвенных нематод в естественных условиях была выделена условная

площадка на правом берегу р. Томи, разделенная на однородные квадраты, которые были загрязнены следующими дозами внесения нефти, бензина с концентрациями 50; 100; 200 г/кг и дизельного топлива 50; 100 г/кг. Параллельно использовалась аналогичная условная площадка с незагрязнённой почвой. Нефтепродукты вносились равномерно по почвенному профилю, на одинаковую глубину.

Выделения нематод, проходило с помощью модифицированного метода Бермана. Основа метода: пробирка, фиксатор ТАФ (триэтаноламин, формалин, вода – 2:7:91) или формалин (4%), термометр, водяная баня. Выдержка выделения нематод составляет 2 суток. Численность нематод рассчитывалась на 100 г сырой почвы. Определение рода нематод осуществляли с помощью цифрового микроскопа Motic DM-BA300 с увеличением $\times 40$ [3].

После предварительной статистической обработки полученных результатов, данные по динамике численности почвенных нематод с концентрациями нефти, бензина: 50; 100; 200 г/кг и концентрациями 50; 100 г/кг дизельного топлива представлены на рисунке 1.

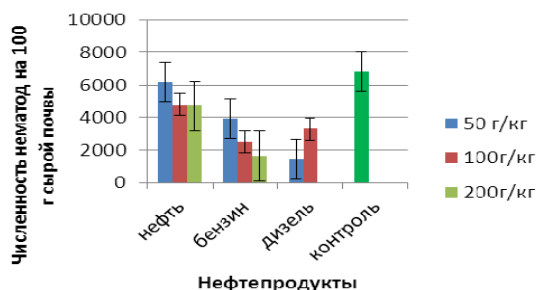


Рис. 1. Динамика численности почвенных нематод в зависимости от концентраций 50; 100; 200 г/кг нефти, бензина и дизельного топлива

Анализ данных, представленных на рис. 1, позволяет выявить особенности влияния нефтезагрязнений на почвенных нематод в зависимости от концентрации. Анализируя исходные данные с контрольными значениями можно выявить следующие изменения. Численность почвенных нематод при загрязнении нефти 50 г/кг фактически не изменилась. В контрольных условиях численность почвенных нематод составляет 6793 экз/100 г сырой почвы. С увеличением концентрации нефти 100 и 200 г/кг, численность почвенных нематод уменьшилась. Численность почвенных нематод при загрязнении бензина 50 г/кг значительно ниже численности нематод контрольных условий. С увеличением концентрации бензина 100 и 200 г/кг численность сообщества нематод уменьшилась в 1,5 раза. Численность почвенных нематод при

загрязнении дизеля 50 г/кг является наименьшей из всех представленных нефтепродуктов концентрации 50 г/кг. После увеличения концентрации дизеля до 100 г/кг выявлено, что численность нематод по сравнению с концентрацией дизеля 50 г/кг увеличилась на 2353 экз/100 г сырой почвы.

Таким образом, на основании проведённых исследований по воздействию нефтепродуктов на сообщество почвенных нематод можно сделать следующие выводы:

1. Повышенное количество углеводов нефти расширяет питательные ресурсы, приводит к активации почвенных микробиологических процессов. При увеличении концентрации нефти проявляется ее токсическое влияние, приводящее к снижению общей численности почвенных нематод;

2. Выявлено токсическое действие бензина при исследуемых концентрациях на сообщество почвенных нематод. При равных дозах внесения концентраций 50; 100; 200 г/кг, бензин приводит к наибольшему уменьшению численности сообщества почвенных нематод в сравнении с другими исследуемыми нефтепродуктами;

3. Показано, что в зависимости от концентрации дизельного топлива происходит изменение структуры почвенных сообществ нематод.

ЛИТЕРАТУРА

1. Соловьёва Г.И. Экология почвенных нематод. – Л.: Наука. – 1986. – 247 с.
2. Н.А. Залялетдинова, С.А. Антропова, А.Г. Карташев. Влияние нефтезагрязнений на сообщество почвенных инфузорий и нематод в лабораторных // Вестник ВГУ, Сер.: Химия. Биология. Фармация. – 2016, № 2. – С. 6.
3. Сушук А.А., Груздеева Л.И. Сообщества почвенных нематод в условиях загрязнения среды // ТМ: Петрозаводск, 2012. – С. 29–32.
4. Шамраев А.В., Шорина Т.С. Влияние нефти и нефтепродуктов на различные компоненты окружающей среды: ОГУ, Оренбург, 2009. – С. 642–645.

ВЛИЯНИЕ БЕНЗИНА НА ПРЕСНОВОДНЫХ РАЧКОВ *DAPHNIA MAGNA*

Т.Е. Лушникова, студентка; А.П. Шкарупо, аспирант

*Научный руководитель Денисова Т.В. доцент каф. РЭТЭМ, к.б.н.
г. Томск, ТУСУР, каф. РЭТЭМ, ltelte100@gmail.com*

D.magna являются одним из лучших тест – объектов так как их жизнь не продолжительна и разведение синхронизированных культур безо всяких затруднений можно произвести в лабораторных условиях. *D.magna*, в течении своей жизни очень резко реагируют на различные

примеси как в лабораторных растворах так и природных водоемах в и в связи с этим они широко используются в биотестировании [1]. Острое токсическое действие исследуемой воды на дафний устанавливается по их смертности (летальности) за определенный период экспозиции. Критерием острой токсичности служит гибель 50 % и более дафний за 48 часов в исследуемой пробе при условии, что в контрольном эксперименте все рачки сохраняют свою жизнеспособность. В экспериментах по определению острого токсического действия устанавливаются: · среднюю летальную концентрацию отдельных веществ (кратность разбавления вод, содержащих смеси веществ), вызывающую гибель 50 % и более тест-организмов (ЛК50-48, ЛКР50-48); безвредную кратность разбавления вод, водных вытяжек, вызывающую гибель не более 10% тест-объектов за 48-часовую экспозицию (БКР10-48) [2].

Целью работы являлось изучение влияния бензина на выживаемость и развитие рачков *Daphnia magna*.

Отлов *D.magna* происходил при помощи стеклянной трубки, опущенной в сосуд с синхронизированной культурой и забором через эту трубку вместе с водой, переносим в колбы для эксперимента. Подсчет *D.magna* в колбах происходит каждые сутки т.е. через 24 часа, через 48 часов, 72 часа, и соответственно 96 часов. Во время эксперимента кормление объекта не производилось. В опытах использовались рачки третьего поколения. Кормом для них служили сухие дрожжи. В банки с ёмкостью 1 литр, отсаживалось по 10 рачков в контрольную и концентрированную воду. Далее в каждую банку вносились концентрации 0,2; 0,4; 0,8 мл/л. Опыт проводился до установления 50% гибели особей в каждой концентрации. Далее проводился сравнительный анализ динамики численности различных концентраций по отношению к друг другу и контрольной емкости.

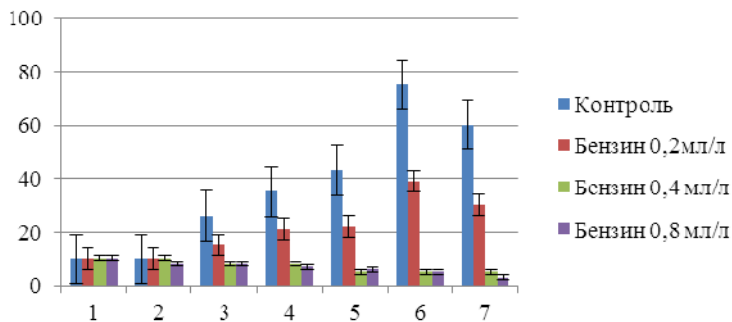


Рис. 1. Динамика численности дафний при концентрации 0,2, 0,4, 0,8 мл/л

При концентрации 0,2 мл/л с 3-их по 6-е сутки наблюдалось увеличение численности дафний, по сравнению с контролем, скорость размножения отличалась, морфологических изменений не выявлено. Для концентрации 0,2 мл/л характерна умеренная степень токсичности – 0,4. При 0,4 мл/л LD₅₀ наступила на 5-е сутки. Выявлено снижение двигательной активности. Размножение и развитие рачков не наблюдалось. Степень токсичности – 0,8, указывает на высокую степень токсичности воды. При концентрации 0,8 мл/л LD₅₀ отмечена на 6-е сутки, также как при концентрации 0,4 мл/л, выявлено нарушение в двигательной активности, развитии и размножении. Концентрация характеризуется высокой степенью токсичности – 0,81.

Таким образом, смертность 50% особей пресноводных рачков *Daphnia magna* происходила при установлении высокой степени токсичности воды, когда индекс токсичности воды (Т) составлял значение большее 0,71. Это свидетельствует о том, что дафнии данного вида неустойчивы к водной среде с высокой степенью токсичности. Ухудшение двигательной активности, вследствие действия токсического эффекта бензина при концентрациях 0,4 и 0,8 мл/л отмечено на вторые сутки и третьи сутки. Необходимо отметить, что коловратки более устойчивы к нефтезагрязнениям по сравнению с дафниями [3].

ЛИТЕРАТУРА

1. Подобина В.М. Фораминиферы и биостратиграфия верхнего сенома на северного района западной сибери // Вестник ТГУ. – Томск. – 2012. – 7 с.
2. Брагинский Л.П. К методики токсикологического эксперимента с тяжелыми металлами на гидробионтах /Л.П., Брагинский, П.Н. Линник. – М., 2003. – 58 с.
3. Карташев А.Г., Влияние нефтезагрязнений на коловраток.

ИССЛЕДОВАНИЕ ПАРАМЕТРОВ МИКРОКЛИМАТА В КОМПЬЮТЕРНЫХ КЛАССАХ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

А.С. Мишенева, студентка

Научный руководитель М.В. Соболева, ст. преп.

г. Ханты-Мансийск, ЮГУ, mpasechnik@yandex.ru

Переносимость человеком температуры и его теплового ощущения в значительной мере зависят от влажности и скорости окружающего воздуха. Чем больше относительная влажность, тем меньше испаряется пота в единицу времени и тем быстрее наступает перегрев организма [1].

Тема является актуальной, потому что параметры микроклимата оказывают непосредственное влияние на тепловое самочувствие человека и его работоспособность. Высокая температура воздуха способствует быстрому утомлению работающего, может привести к перегреву тепловому удару или профзаболеванию. Низкая температура может вызвать местное или общее охлаждение организма, стать причиной простудного заболевания. Высокая относительная влажность воздуха при высокой температуре способствует перегреву организма. При низкой – усиливает теплоотдачу с поверхности кожи, что ведет к переохлаждению организма. Низкая влажность вызывает пересыхание слизистых оболочек дыхательных путей. Подвижность воздуха эффективно воздействует теплоотдаче организма человека. Она положительна при высоких температурах и отрицательна – при низких [4].

Цель работы – измерить параметры микроклимата двух компьютерных классов с ЖК-мониторами, ЭЛТ-мониторами и сравнить их с требованиями нормативно-технической документации.

Исследования проводились в двух компьютерных классах Югорского Государственного Университета. Компьютерный класс № 1 содержит 15 компьютеров, из них 5 с ЖК-мониторами, остальные с ЭЛТ-мониторами. В помещении 15 светильников, из них 4 над доской, расположены перпендикулярно рабочему столу. Компьютерный класс №2 содержит 9 компьютеров с ЖК-мониторами. В помещении 14 светильников, из них 4 над доской, расположены параллельно рабочему столу. Полученные данные в ходе исследований представлены в табл. 1, 2.

Т а б л и ц а 1

Полученные данные в ходе исследований (до проветривания помещения)

Параметры	Показатели компьютерного класса №1	Показатели компьютерного класса №2	Нормативные показатели СанПиН 2.2.2/2.4.1340-03
Компьютерный стол:			
длина, см	60	72	
ширина, см	120	122	80–140
высота, см	75	76	52–76
Освещенность, Еиск, лк	390	434	300–500 лк
Относительная влажность, %	55,2	56,3	55–62
Температура, °С	21	20	19–21
Скорость движения воздуха, м/с	0,01	0,01	< 0,1
Напряженность ЭП, В/м	24	2	25

**Полученные данные в ходе исследования
(после проветривания помещения)**

Параметры	Показатели компьютерного класса №1	Показатели компьютерного класса №2	Нормативные показатели СанПиН 2.2.2/2.4.1340-03
Относительная влажность, %	55	55,4	55–62
Температура, °С	20	19	19–21
Напряженность ЭП, В/м	22	3	25

В ходе исследовательской работы использовались следующие измерительные приборы [1]:

1. Измеритель температуры и влажности «ТКА-ТВ».
2. Прибор Люксметр «ТКА-Люкс» предназначен для измерения освещенности, создаваемой различными источниками, произвольно пространственно расположенными, в лк.
3. Термоанемометр ТКА-СДВ предназначен для измерения скорости движения воздуха внутри помещений в диапазоне окружающих температур от 0 до 50°С.
4. ПЗ-50В – измеритель напряженности поля промышленной частоты.

В соответствии с СанПиН 2.2.2/2.4.1340-03 можем сравнить нормированные показатели с полученными показателями. Относительная влажность воздуха в компьютерном классе № 1 равна 55,2%, в компьютерном классе № 2 равна 56,3%, а нормированный показатель в пределах от 55 до 62%. Температура воздуха в компьютерном классе № 1 равна 21 °С, в компьютерном классе № 2 равна 20°С, а нормированный показатель в предел от 19 до 21 °С. Напряженность электрического поля в помещении компьютерного класса № 1 равна 24 В/м, в помещении компьютерного класса № 2 равна 2 В/м, а нормированный показатель напряженности электрического поля в диапазоне частот 5 Гц – 2 кГц равен 25 В/м.

Стоит отметить, что в компьютерных классах присутствует система вентиляции, что необходимо для создания оптимальных параметров микроклимата.

Вывод: на основании проделанных измерений можно сказать, что показатели двух компьютерных классов не многим отличаются друг от друга и по всем показателям соответствуют СанПиН.

ЛИТЕРАТУРА

1. Айзман Р.И., Шуленина Н.С., Ширшова В.М.: Основы безопасности жизнедеятельности. – 2010. – 247 с.
2. Осьмушка К.С. Исследование параметров микроклимата в компьютерных классах // ЮГУ, 2014. – 44–48 с.
3. СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организация работы».
4. Чулков Н.А. Безопасность жизнедеятельности. – Томск: ТПУ, 2010. – 180 с.

ВЛИЯНИЕ БЕНЗИНА НА АКВАРИУМНЫХ РЫБ *POECILIA RETICULATE*

Е.Р. Моргунова, студентка; А.П. Шкарупо, аспирантка
Научный руководитель А.Г. Карташев, д.б.н., проф. каф. РЭТЭМ
г.Томск, ТУСУР, Ekaterina_mg97@mail.ru

Ранний онтогенез рыб является периодом жизненного цикла, в течении которого организм наиболее подвержен влиянию внешних факторов. Молодь гуппи *Poecilia reticulata* можно рассматривать в качестве биоиндикаторов изменений, происходящих в водной среде под влиянием загрязнителей.

Исследования проводились на живородящих гуппи – *Poecilia reticulata* в возрасте не старше 2 суток (24–48 ч). Для содержания гуппи используют термостатированные аквариумы, обеспечивающие плотность посадки тест-объектов из расчета 1–2 дм³ воды на 1 экземпляр, производителей – не менее 4 дм на 1 экземпляр. Аквариум заполняли, отстоянной в течение 7 суток, водопроводной водой. С периодичностью в три дня, проводили частичную замену воды, около 25%. Наиболее благоприятный температурный режим в пределах 24–27 °С.

Кормление гуппи осуществлялось один раз в сутки, прикорм производителей проводили до двух раз в сутки. Кормом служили: универсальный хлопьевидный корм для рыб «Tetra Min» и живые ракообразные *Artemia salina*. Корм вносили в таком количестве, чтобы рыбы съедали его без остатка за 3–5 мин, так как излишки приводят к ухудшению качества воды в аквариуме.

Самцов и самок рекомендуется содержать в отдельных аквариумах. При совместном содержании самцы растут медленнее и имеют меньшие размеры. Самцы, как правило, мельче (3–4 см) и имеют более яркую окраску, чем самки. У них преобладают серовато-коричневые тона с очень яркими красными, голубыми, зелеными и черными

пятнами. Самки больше самцов, до 6 см в длину, чаще желтовато-зеленые. Анальный плавник у самок округлый. У молодых самцов он имеет ту же форму, но со временем, в период полового созревания, он начинает удлиниться и превращается в подвижный гоноподий.

Для получения молоди отбирают производителей не старше двух лет (продолжительность жизни гуппи в аквариумных условиях 3–3,5 года) и за три дня до постановки опытов помещают в общий аквариум для спаривания. Соотношение самцов и самок 2:1. Необходимо учитывать, что однажды оплодотворенная самка может нереститься несколько раз. Самку готовят к нересту, помещая в отдельную термостатированную нерестовую емкость объемом не менее 4 дм³. Готовность самки к вымету мальков определяют по наличию хорошо заметного темного пятна перед анальным плавником. При этом форма брюшка приближается к прямоугольной и оно становится намного шире спины. После окончания нереста самок изолируют, так как они поедают потомство. Мальки рождаются совершенно сформированными. Лучшим кормом для них является «пыль», состоящая из представителей разных морских организмов: инфузорий, коловраток, молоди ветвистоусых рачков и науплиусов веслоногих рачков. По мере роста в рацион рыб вводят измельченный трубочник, мотыль, и другой живой корм.

Эксперимент был начат спустя несколько часов после родов, в аквариум с 10-ю особями внесен бензин, концентрация которого составляла 0,1 мл/л. Следующая концентрация объемом 0,3 мл/л внесена, где насчитывалось так же 10 мальков. По прошествии 2-х суток для контроля был выбран аквариум с 10 рыбами в качестве контроля. Внесена концентрация 0,5 мл/л в аквариум с рожденными на несколько часов позже мальками. Наибольшая концентрация объемом 0,8 мл/л. В течении данного опыта мальки 3х концентраций не значительно отставали в развитии, но выявлены некоторые аномалии развития: нарушение формирования внутренних органов, туловища, плавников, наблюдались искривления позвоночников, незначительные воспаления в области дыхательных путей. Особи служившие контролем, развивались быстрее относительно рыб с концентрациями бензина 0,1, 0,3 и 0,5 мл/л. При концентрации 0,8 мл/л мальки через час после внесения данного вещества приобрели более светлый окрас, что свидетельствовало о явной интоксикации организма, нарушилась координация движений, наблюдалось сокращение потребления пищи LD50 наступила на 7-е сутки.

На основании проведенного исследования по влиянию бензина на гуппи *Poecilia reticulata* можно сделать следующие выводы:

1. При незначительных концентрациях, бензин вызывает такие нарушения как: искривления позвоночника, деформации головного отдела и плавников, замедление общего развития организма.

2. Выжившие половозрелые особи Гуппи, ранее подверженные влиянию бензина, имеют такие аномалии как: раскол плавника; темное пятно в области дыхательных путей, ослаблена иммунная система, что ведет к различным заболеваниям. У самок отмечено рождение мертвого потомства.

3. При повышении концентраций растет число погибших особей.

ЛИТЕРАТУРА

1. Пряжевская Т.С., Черкашин С.А. Влияние нефтеуглеводородов на ранний онтогенез рыб // Известия ТИНРО (Тихоокеанского науч.-исслед. рыбохозяйственного центр). – 2007. – Т. 149. – С. 359–365.

2. Анисимова, И.М. Лавровский В.В. Ихтиология. Основные звенья жизненного цикла рыб. Размножение и развитие рыб // Ихтиология: Из-во Высшая школа. – 1983 [Электронный ресурс]. – Режим доступа: http://zoomet.ru/ixt/ixtiolog_79.html (дата обращения: 02.02.2018).

3. Каниева Н.А. Физиологические механизмы адаптации рыб к влиянию каспийской нефти: автореф. дис. ... д-ра биол. наук. – Астрахань, 2004. – 48 с.

4. Карташев А.Г. Биоиндикация экологического состояния среды: учеб. пособие. – Томск: ТУСУР, 2012. – 58 с.

ИССЛЕДОВАНИЕ ВЛИЯНИЯ СПЕКТРОВ СВЕТА НА РОСТ И РАЗВИТИЕ РАСТЕНИЙ

А.А. Мороз, П.В. Тимошенко, студентки

Научный руководитель Е.Г. Незнамова, доцент каф. РЭТЭМ, к.б.н.

г. Томск, ТУСУР, каф. РЭТЭМ, univerh66@mail.ru,

moroz2010_95@mail.ru, timoshenko-polya.v@yandex.ru

*Проект ГПО РЭТЭМ-1403 «Исследование влияния света
на тепличные растения»*

В настоящее время существует огромное количество методик, направленных на увеличение урожайности сельскохозяйственных культур. Так в начале XX в. было замечено благоприятное воздействие искусственного освещения на рост растений [1].

Целью данной работы являлось изучение материалов по предпосевной обработке и проведение теоретического анализа по различным спектрам светодиодных ламп.

Для осуществления данной цели необходимо было выполнить следующие задачи:

1. Провести обзор методик по предпосевной обработке;
2. Выполнить теоретический анализ по спектрам светодиодных ламп на основе найденных источников.

Досветка овощных культур в определенной области спектра, позволяет существенно повысить их урожайность [2]. Известно, что растения в процессе фотосинтеза поглощают спектр только определенных длин волн [3].

Для растений физиологическое активное излучение, при котором происходит фотосинтез, колеблется в пределах от 300 до 800 нм, а спектр поглощения фотосинтетической активной реакции (ФАР) – в интервале 400–700 нм.

Особенности воздействия разных участков спектра на растения определяются длинами волн.

«Синий свет» 400–500 нм, 5200–6500 К – «дневной» свет / Daylight необходим для фотосинтеза и регуляции (содержит пигмент криптохром). Необходим для вегетативной стадии роста, в целом способствуя укреплению растений, развитию корневой системы, стебля, листьев [4].

«Красный свет» 600–700 нм, 2700–3000 К – «теплый» свет / Warmlight – имеет ярко выраженное действие на фотосинтез, развитие и регуляцию процессов цветения и плодоношения [3, 4].

«Зеленый свет» 500–600 нм, 4000–4200 К – «холодный» свет / Coollightne является абсолютно необходимым для обеспечения фотосинтеза растений, но благодаря своей высокой проникающей способности полезен для обеспечения фотосинтеза оптически плотных листьев [2, 4].

Ближнее инфракрасное излучение 780–1100 нм, оказывает сильное формообразовательное влияние на растение, которое проявляется в растяжении осевых органов (стебель, подсемядольное колено).

Немаловажным фактором в обеспечении высоких урожаев является совершенствование технологий предпосевной обработки семян.

Предпосевная обработка дает возможность вывести посевной материал из состояния покоя, стимулировать дальнейший рост и развитие растений, а так же защитить их от возбудителей болезней.

В наши дни в сельскохозяйственных разработках выделяют три основных метода: физический, химический и биологический [5].

Принцип действия физических методов основан на использовании электрических, электромагнитных, магнитных, тепловых полей, лазерного облучения, оптического облучения инфракрасными (ИК) и ультрафиолетовыми лучами (УФ) [5, 6]. А так же на применении различных способах стимулирующего воздействия на семена, в том числе, интенсивным концентрированным солнечным светом, монохроматическим видимым светом, низкоинтенсивным когерентным излуче-

нием, сверхвысокочастотным воздействием, лазерным облучением, стимуляторами роста [7].

В основу действия светодиодного матричного аппарата «Дюна-Т» положен биологический эффект двухфакторного воздействия красного и инфракрасного света. «Дюна-Т» обладает явлением фото-биоактивации, возникающим в результате взаимодействия красного и инфракрасного излучения с живой клеткой. Оптическое излучение, представляет собой экологически чистые виды электромагнитных излучений, применяемые с целью восстановления функционирования клетки, ткани, биологической системы в целом [8]. На основании вышесказанного формируется представление, что обработка семян овощных культур оптическим излучением красного и инфракрасного (ИК) спектра света является одним из перспективных методов для реализации технологий предпосевной стимуляции семенного материала.

ЛИТЕРАТУРА

1. Астафурова Т., Лукаш В., Гончаров А., Юрченко В. Фитотрон для светодиодной досветки растений в теплицах и на дому // Полупроводниковая светотехника. – 2010. – № 3. – С. 36–38.
2. Нишпорович А.А. Фотосинтетическая деятельность растений и пути повышения их продуктивности. Теоретические основы фотосинтетической продуктивности. – М.: Наука, 1972. – 511 с.
3. Козинский В.А. Электрическое освещение и облучение. – М.: Колос, 1991. – 239 с.
4. Тихомиров А.А., Шарупич В.П., Лисовский Г.М. Светокультура растений в теплицах [Электронный ресурс]. – Новосибирск: Изд-во СО РАН, 2000. – Режим доступа: <http://www.greenhouses.ru/Svetokultura>.
5. Спиридонов А.Б. Исследование и разработка электрофизической технологии дражирования семян льна-долгунца: дисс.... канд. техн. наук. – Ижевск, 2014.
6. Бекузарова С.А., Беляева В.А. Повышение всхожести твердых семян клевера // Евразийский союз ученых (ЕСУ). – 2015. – № 17 (29.08.2015) [Электронный ресурс]. – URL: <http://euroasia-science.ru/selskoxozyajstvennyenauki/povyshenie-vsxozhести-tverdyx-semyan-klevera/> (дата обращения: 22.02.2018).
7. Ludwig H. Die Kemruhe der Gramineen und ihre Problematik bei der Saatgutuntersuchung unter besonderer Berücksichtigung des Einsatzes von Gibberellinsäure / Proc. ISTA, 36, 1971. – № 2. – P. 289–305.
8. Серых Б.Т., Чехова З.А., Новикова С.В. Светодиодная фототерапия аппаратом «Дюна-Т» заболеваний суставов / ЗАО «Медико-экологический центр «Дюны» [Электронный ресурс]. – Режим доступа: <http://www.dunya.ru/> (дата обращения: 30.02.18).

ВЛИЯНИЕ НЕФТЕПРОДУКТОВ НА МОЛЛЮСКОВ

К.И. Мурадян, студент, А.П. Шкарупо, аспирант

*Научный руководитель Т.В.Денисова, доцент каф. РЭТЭМ, к.б.н
г. Томск, ТУСУР, kanakara.muradyan@mail.ru*

Проблема загрязнения природной среды, в том числе и водоемов, остается одной из наиболее актуальной в современном индустриальном обществе [1].

Пресноводные моллюски представляют собой таксономический разнообразную, экологически пластичную и весьма широко распространенную группу гидробионтов, роль которых в жизни пресноводных экосистем огромна. Без изучения моллюсков невозможно ни комплексное исследование континентальных водоемов, ни решение таких важнейших практических задач, как оценка рыбохозяйственного значения водоемов, биомониторинг [2].

Объектом исследования является моллюски (Planorbis) – брюхоногие моллюски, средой обитания которых являются пресноводные водоемы., Раковина у моллюсков имеет дисковидную форму, все завитки находятся в одной плоскости, при этом они не приподняты над устьем. Если высушить прудовика, вес его раковины составит 80%, то есть мягкие ткани составляют всего 20%, а вот у катушки вес раковины составляет 91%, а вес всего тела – только 9%. Довольно часто катушек содержат в аквариумах вместе с рыбками. Эти моллюски выделяют меньше слизи, чем прудовики, потому они не умеют ползать по поверхности воды. Кожное дыхание у них играет не большую роль, в сравнении с прудовиками [3].

Для наблюдения было взято три аквариума, с добавлениями концентраций нефти 1, 4 мл/л и 0 (контроль). В каждом находилось по 8 особей. Питанием служили зеленые водоросли. В результате исследования, длившееся 12 дней, наблюдались изменения в численности улиток, которые представлены в таблице. Так же изменения в поведении, менялась двигательная активность, их расположение, движение усиков, питание.

Анализ данных в представленной таблице позволил заметить, что концентрация нефтезагрязнения равная 1 мл/л, оказывает влияние на 12 день после действия нефтезагрязнения. При 4 мл/л наблюдается сокращение численности в 2 раза, что фактически является критичным уровнем загрязнения. В дальнейшем численность не изменялась.

Вывод. На основании проведенных исследований можно считать, концентрация нефтезагрязнения равная 8 мл/л является критической для выживаемости моллюсков. Полученные результаты могут быть методом разработки биоиндикации.

Изменение численности моллюсков катушек

Сутки	1 мл/л	4 мл/л	0 мл/л (контроль)
1-е	8	8	8
2-е	8	8	8
3-и	8	8	8
4-е	8	8	8
5-е	8	8	8
6-е	8	4	8
7-е	8	4	8
8-е	8	4	8
9-е	8	4	8
10-е	8	4	8
11-е	8	4	8
12-е	6	4	8

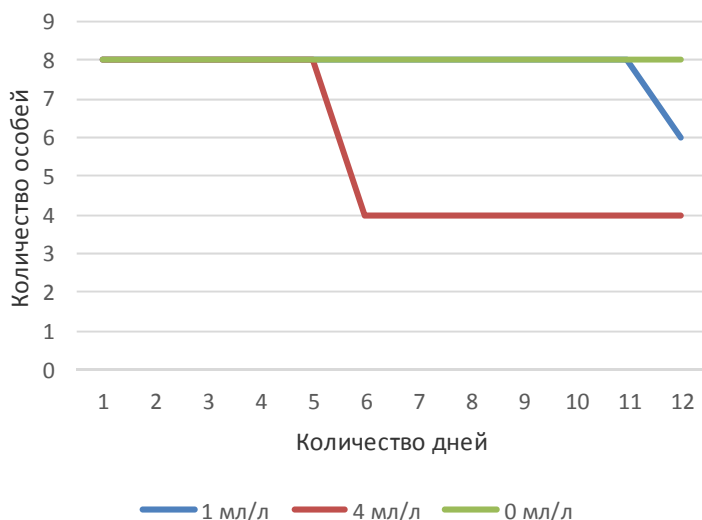


Рис. 1. Изменение численности улиток при разных концентрациях

ЛИТЕРАТУРА

1. Карташев А.Г. Экологические аспекты нефтедобывающей отрасли Западной Сибири. Томск: ТУСУР, 2007. – 218 с.
2. Бедова П.В., Колупаев Б.И. Использование моллюсков в биологическом мониторинге состояния водоемов // Экология. – 1998. – № 5.
3. Улитка Катушка. [Электронный ресурс]. – Режим доступа: URL: <http://aquaplantfish.narod.ru/mollusk/katushka/katushka.htm> (дата обращения: 24.02.2018).

4. Долгин В.Н. К изучению пресноводных моллюсков Сибири // Вестник Томского гос. педаг. ун-та – 2009. – №11. С. 174–178.

5. Карташев А.Г. Адаптация животных к хроническим факторам // LAP LAMBERT Academic Publishing, Saarbrücken, 2014. – 260 с.

РАЗРАБОТКА И АПРОБАЦИЯ ЭЛЕКТРОННОГО КУРСА «ОБУЧЕНИЕ ОХРАНЕ ТРУДА»

А.С. Шумилова, студент

*Научный руководитель С.А. Полякова, доцент каф. РЭТЭМ, к.н.,
д.б.н.*

г. Томск, ТУСУР, каф. РЭТЭМ, ur.alexsilver@gmail.com

Статьей 225 Трудового кодекса Российской Федерации предусмотрено обязательное обучение по охране труда работников, руководителей организаций и работодателей – индивидуальных предпринимателей и проверка знаний требований охраны труда [1].

Зачастую организации прибегают к услугам сторонних обучающих организаций, аккредитованных в соответствии с Приказом Минздрава от 01.04.2010 г. №205н «Об утверждении перечня услуг в области охраны труда, для оказания которых необходима аккредитация, и Правил аккредитации организаций, оказывающих услуги в области охраны труда». В 2014 г. такую аккредитацию, по инициативе кафедры РЭТЭМ, получил ТУСУР, и в связи с этим стало необходимо разработать актуальное учебно-методическое обеспечение курсов для обеспечения конкурентоспособности вуза в этой сфере.

Начальный этап работы над учебно-методическим обеспечением проводился группой проектного обучения «Актуальная нормативно-правовая база в области техносферной безопасности», специально созданной для этой цели на базе кафедры РЭТЭМ. Участники группы собирали и перерабатывали необходимую информацию, учитывая доступные к изучению учебные пособия по охране труда, законодательные акты РФ и различные методические указания. Результатом работы группы стало учебное пособие, состоящее из 4 разделов:

- 1) основы охраны труда;
- 2) основы управления охраной труда в организации;
- 3) специальные вопросы обеспечения требований охраны труда и безопасности производственной деятельности;
- 4) социальная защита пострадавших на производстве.

Однако внедрить достаточно большой объем информации в образовательный процесс было достаточно проблематично.

В последнее время развитие информационных технологий сильно изменило формы взаимодействия в мире, это преобразование так же

коснулось и образовательной среды. Дистанционное образование превратилось в неотъемлемую составную часть образовательной системы развитых стран мира [2]. Необходимость проведения обучения требованиям охраны труда и проверки знаний, обусловленная законодательством, тесно связана с такой проблемой, как отрыв работников от производственного процесса. Потеря рабочих рук может отрицательно сказаться на работе предприятия – этим и обуславливается выбор формы электронного обучения охране труда в ТУСУРе.

Созданный курс был адаптирован для использования в рамках курсов повышения квалификации, а также для применения в таких дисциплинах как «Охрана труда», «Безопасность труда» и смежных с ними.

Курс состоит из вводного тестирования (для определения начальных знаний респондента), четырех разделов с лекционным материалом общим объемом 72 часа и контрольного (итогового) тестирования для определения эффективности курса и поданного материала. Некоторые вопросы в целях контроля в вводном и итоговом тестировании повторялись.

Каждое тестирование состоит из 20 вопросов типа «выбор ответа из предложенного списка». Каждый вопрос оценивался в пять баллов, общая оценка за каждый тест – 100 баллов.

Первая апробация курса проводилась в группе 224 кафедры РЭТЭМ – участие приняло 12 человек. Результаты прохождения вводного и итогового тестирования и их сравнение представлены на рис. 1.

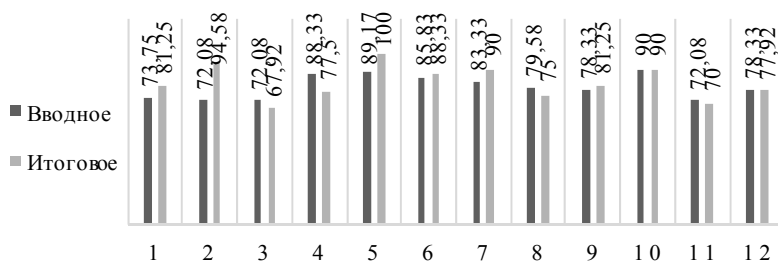


Рис. 1. Результаты первой апробации

У пяти из 12 респондентов результаты вводного тестирования лучше, чем итогового. Возможные причины:

- невнимательное изучение материала;
- материал оказался сложнее и запутаннее, что привело к путанице между имеющимися и полученными знаниями;
- невнимательное чтение вопроса и вариантов ответа.

Контрольные (повторяющиеся) вопросы были под номерами 4, 10, 13, 14, 18, 19. Результаты сравнения среднего значения по ответам представлены на рис. 2.

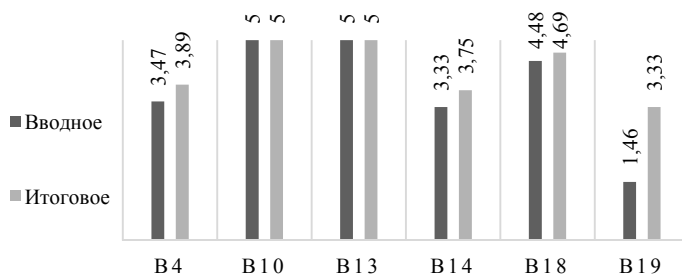


Рис. 2. Средние значения по контрольным вопросам

Как видно из рисунка, средние результаты до и после отличаются в положительную сторону. Если говорить конкретно по каждому рецензенту и каждому вопросу, тут оценки расходятся:

- для первого контрольного вопроса результат улучшился у пяти из 12 рецензентов, у двух результат ухудшился, у оставшихся пяти остался на прежнем уровне;

- у второго и третьего вопроса результаты не изменялись;

- в четвертом вопросе результат стал лучше у двух рецензентов, у восьми не изменился, у одного – ухудшился;

- для пятого вопроса высший балл на итоговом тестировании по сравнению с вводным получило двое тестируемых, у остальных не изменился;

- у последнего контрольного вопроса результаты следующие: верными стали ответы у пяти человек, у семи не изменились.

В целом, итоговые средние баллы лучше вводных, но говорить об эффективности программы пока рано.

Дальнейшие доработка, совершенствование и тестирование курса «Обучение по охране труда» будет производиться в рамках выпускной квалификационной работы.

ЛИТЕРАТУРА

1. «Трудовой кодекс Российской Федерации» от 30.12.2001 № 197-ФЗ (ред. от 03.07.2016), ст. 225 «Обучение в области охраны труда» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_346_83/f184ddd9da693cb68e264dc8dd028748257b9b03/ (дата обращения: 12.03.2018).

2. Дембицкая С.В., Кобылянский А.В. Особенности применения дистанционного обучения при изучении охраны труда // Электронное обучение в непрерывном образовании. – 2015. – Т. 1, №1(2). – С. 52–57.

РАСПРЕДЕЛЕНИЕ ДОЖДЕВЫХ ЧЕРВЕЙ В АНТРОПОГЕННО-НАРУШЕННЫХ ПОЧВАХ

А.А. Тюменцева, студентка

*Научный руководитель Т.В. Денисова, доцент каф. РЭТЭМ
г. Томск, ТУСУР, каф. РЭТЭМ*

Поверхность большей части суши покрыта почвами. Свойства почв наряду с климатическими условиями определяют возможность заселения их той или иной растительностью, а последняя в свою очередь определяет характер населения животных, обитающих в почве и на ее поверхности в данном участке суши.

На педобионтов и на дождевых червей оказывают влияние антропогенно-нарушенные почвы, в том числе содержащиеся в них тяжелые металлы. Тяжелые металлы могут вызывать изменения общей численности почвенных микроорганизмов. Целью исследования явилось изучение численности, биомассы и видового состава дождевых червей в районах с различной антропогенной нагрузкой на территории г. Томска Кировского района.

Для достижения цели были поставлены задачи:

1. Выявить изменение численности и биомассы дождевых червей в осенний период.
2. Исследовать видовой состав дождевых червей при различных антропогенных нагрузках на почвы.

В период с 15.09.2017 г. по 15.10.2017 г. был осуществлен количественный и фаунистический сбор дождевых червей методом раскопки. Объектом исследования являются почвы Кировского района города Томска. В настоящее время в г. Томске действуют такие промышленные предприятия, как Томская ТЭЦ-3, Томская ГРЭС-2, ЗАО «Метанол» и ОАО «Томский нефтехимический завод», которые дают около 13,5 тыс. тонн выбросов в год, что составляло более половины всех выбросов загрязняющих веществ в Томске. Среди загрязняющих атмосферу предприятий отмечаются Томсклесдрев, Томсктеплосеть, Томск-авиа, Томь-Аппарель, спичфабрика «Сибирь», ТЗКМиИ, Горэнерго, ТЗРО. В Кировском районе города Томска расположены Томский электротехнический завод, Томский радиотехнический завод, Томский завод светотехники, СибНефтекарт.

В ходе статистического анализа были вычислены – критерий достоверности разности между биомассой и численностью дождевых червей. Данные критерия достоверности разности величин биомассы и численности дождевых червей в почвах исследуемых районов размещены в табл. 1.

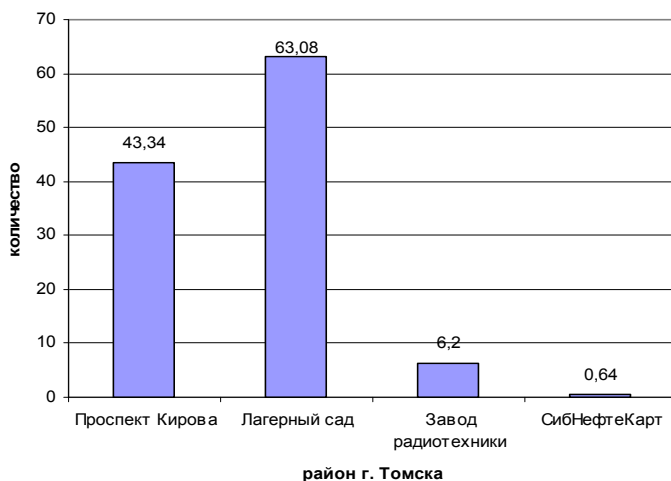


Рис. 1. Биомасса дождевых червей в исследуемых районах за 2017 г.

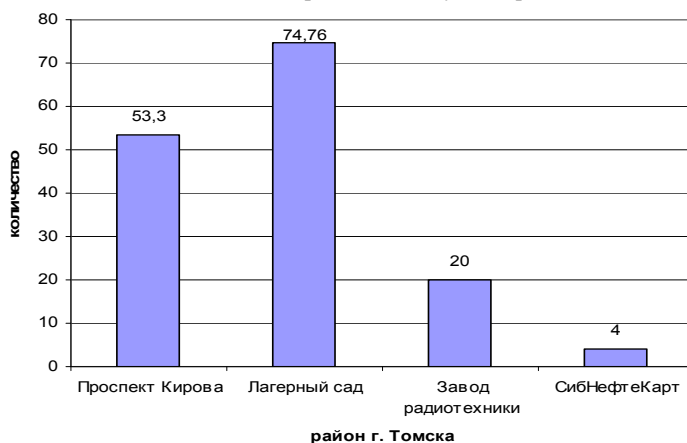


Рис. 2. Численность дождевых червей в исследуемых районах за 2017 г.

Таблица 1

Критерий достоверности разности величин биомассы и численности дождевых червей в исследуемых районах в 2017 г.

Исследуемые районы	Проспект Кирова	Лагерный сад	Завод радиотехники	СибНефтеКарт
Критерий достоверности разности t_d по биомассе	1,7929	3,646	3,676	3,33
Критерий достоверности разности t_d по численности	2,18	5,11	5,21	4,07

Результаты получили следующие: максимальное количество дождевых червей в 2017 г. наблюдалось в парке Лагерный сад и в парке Кирова. При изучении видового разнообразия дождевых червей в г. Томске Кировского района было произведено частичное описание исследуемых участков. Результаты представлены в табл. 2.

Таблица 2

Встречаемость видов дождевых червей в исследуемых районах

Виды дождевых червей	Лагерный сад	проспект Кирова	Завод радиотехники	Сибнефтекарт
<i>Aporrectodea caliginosa</i>	22	11	3	
<i>Aporrectodea rosea</i>	2	6		2
<i>Aporrectodea longa</i>		1		
<i>Eisenia uralensis</i>	3			2
<i>Eisenia nordensholdti</i>		3	2	
<i>Lumbricus rubellus</i>			2	

Выводы. В результате проведенного исследования изучили численность, биомассу и видовой состав дождевых червей в районах с различной антропогенной нагрузкой на территории г. Томска Кировского района. Выявили изменения численности и биомассы дождевых червей в осенний период. Нами обнаружено 7 видов дождевых червей, которые относятся к различным морфо-экологическим группам и принадлежат к двум морфоэкологическим типам: из первого типа, питающегося на поверхности почвы, выделены подстилочные и почвенно-подстилочные, а из второго типа – собственно почвенных, которые питаются почвенным перегноем, норники и среднеярусные. Нами выявлены различия в видовой структуре и численности дождевых червей в фоновых биоценозах и тех, которые подвержены в разной степени антропогенным нагрузкам, а также в разных типах биогеоценозов, что обусловлено физико-химическими параметрами почв в разных районах г. Томска. Исследование видового состава при различных антропогенных нагрузках показало, что более благоприятная почва для дождевых червей выявлена в двух исследуемых участках: в парке Лагерный сад и Проспекте Кирова, где было обнаружено наибольшее количество и видовой состав дождевых червей. Изменение условий окружающей среды сказываются не только на численности и биоразнообразии почвенной мезофауны, но и на сезонные колебания их биомасс.

ЛИТЕРАТУРА

1. Алексеев Ю.В. Тяжёлые металлы в почвах и растениях. – Л.: Агропромиздат. Ленингр. отделение, 1987. – 142 с.

2. Амирджян Ж.А. Содержание тяжёлых металлов в загрязнённых почвах // Химия в сельском хозяйстве. – 1994. – № 4. – С. 26–28.
3. Балув В.К. Дождевые черви основных почвенных разностей Ивановской области // Почвоведение. – 1950. – № 4. – С. 219–227.
4. Гиляров М.С. Почвенные беспозвоночные как объект экологического мониторинга / М.С. Гиляров, А.Д. Покаржевский // Охраняемые природные территории. – М.: Центр международных проектов ГНТ, 1983. – С. 108–115.
5. Гиляров М.С. Учёт крупных почвенных беспозвоночных (мезофауны) // Методы почвенных зоологических исследований. – М.: Наука, 1975. – С. 12–29.
6. Горбатов В.С. Трансформация соединений и состояние цинка, свинца и кадмия в почвах: автореф. ... дис. канд. биол. наук. – М., 1983. – 24 с.

ОПРЕДЕЛЕНИЕ КАЧЕСТВА ВОДЫ В ГЛАВНОМ И УЧЕБНО-ЛАБОРАТОРНОМ КОРПУСАХ ТУСУРА

**Д.А. Коршунова, А.А. Заздравных, Ю.С. Кудрякова, А.О. Ким,
Н.А. Конгирович, К.В. Синцев, студенты**

Научный руководитель С.А. Полякова, доцент каф. РЭТЭМ, к.б.н.

г.Томск, ТУСУР, каф. РЭТЭМ, cappwho@gmail.com

*Проект ГПО РЭТЭМ-1702 «Экологические исследования водных
ресурсов»*

Загрязнение питьевой воды – это очень актуальная проблема, остро стоящая перед человечеством. Согласно данным Всемирной организации здравоохранения, на нашей планете чистой питьевой воды, которую можно было бы употреблять без предварительной очистки, осталось всего один процент. А ведь из-за употребления некачественной воды наносится огромный вред организму.

Причин, по которым происходит загрязнение, может быть очень много. Но самая основная – это непосредственно источник воды. Но даже сами источники могут загрязняться различными способами [1].

Томская область оказалась на последнем месте в рейтинге по показателям качества питьевой воды в регионах страны. По данным рейтинга, из 524 источников и водопроводов в Томской области 426 не отвечают санитарным нормам. Низкое качество питьевой воды объясняется недостаточной защищенностью источников воды (61 объект) и нарушением очистки воды в системах водоканала (418 объектов). Доля водопроводов, не соответствующих нормам, составляет 81,3% – это худший показатель по России.

Наряду с Томской областью аутсайдерами рейтинга стала Хакасия (80,6%), Чеченская Республика (75,4%) и Тюменская область (57,5%). По мнению составителей исследования, самую чистую питьевую воду можно найти в Санкт-Петербурге и Республиках Мордовия,

Адыгея, Ингушетия. В этих регионах источники и водопроводы, не соответствующие санитарным нормам, обнаружены не были [2].

Город Томск – один из крупнейших промышленных центров Западной Сибири. Исследования свидетельствуют о высоком уровне химического и микробиологического загрязнения воды, в основном из-за сброса неочищенных производственных и бытовых стоков.

Вода состоит не только из воды, но и из множества примесей, не видимых невооруженным глазом. Источниками минерализации воды являются различные неорганические соли и минералы, иногда и некоторые органические соединения. В связи с такой острой проблемой, наша группа провела исследование качества воды в Главном и Учебно-лабораторном корпусах ТУСУРа. Забор и измерения воды проводились 3 раза в неделю в течение месяца с помощью тестера Xiaomi-TDS, он умеет проверять качество воды на содержание: ионов кальция, магния, сульфатов, хрома, цинка, свинца и меди.

Полученные данные показали, что в период с февраля по март качество воды изменяется, но не в значительном диапазоне. Первые данные составляли 235 мг/л в ГК, 249 мг/л в УЛК, последние 255 мг/л в ГК, 281 мг/л в УЛК (рис. 1).

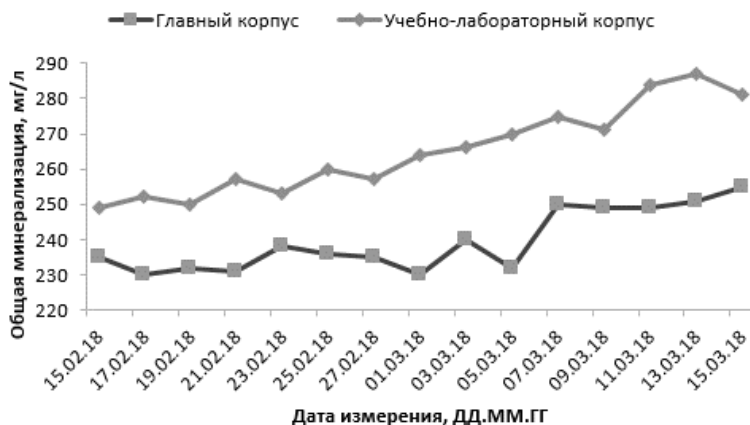


Рис. 1. Полученные данные по качеству воды в ГК и УЛК

В ходе проведенного исследования можно сделать следующие выводы:

1. В приведенном графике мы наблюдаем незначительные изменения данных, это может быть связано с очисткой и промывкой водопроводных труб.

2. Согласно СанПиН № 2.1.4.1074-01, вода считается пригодной для питья, ее минерализация соответствует значению до 1000 мг/л [3].

ЛИТЕРАТУРА

1. Официальный сайт компании Best Water Technology (BWT) [Электронный ресурс]. – Режим доступа: <http://www.bwt.ru/useful-info/985/> (дата обращения: 01.03.2018).

2. Официальный сайт ГИС ЖКХ [Электронный ресурс]. – Режим доступа: <https://dom.gosuslugi.ru/#!/map/water-quality> (дата обращения: 03.03.2018).

3. Гигиенические требования к качеству воды централизованных систем питьевого водоснабжения [Электронный ресурс]. – Режим доступа: <http://docs.cntd.ru/document/901798042> (дата обращения: 04.03.2018).

ВЛИЯНИЕ НЕФТЕЗАГРЯЗНЕНИЙ НА УЛИТОК ФИЗА (PHYSA)

Т.Н. Андреева, студентка; А.П. Шкарупо, аспирант

*Научный руководитель Т.В. Денисова, доцент каф. РЭТЭМ, к.н.
г.Томск, ТУСУР, testacea@yandex.ru*

Проблема загрязнения водоемов остается одной из наиболее актуальной в Западной Сибири [1]. Моллюски представляют собой таксономически разнообразную, экологически пластичную и распространенную группу гидробионтов. Без изучения моллюсков затруднено комплексное исследование континентальных водоемов, решение важнейших практических задач, биомониторинга. Установлено, что выживаемость моллюсков в загрязненной воде нефтью изменяется в зависимости от концентрации загрязняющего вещества [2].

Объектом исследования являются моллюски – отряд лёгочные моллюски, подотряд сидячеглазые, семейство физида. Представители этого семейства обладают раковинами, завитыми в левую сторону [3]. Раковина шириной до 6 мм, а высотой до 10 мм, яйцевидной форму, 3–4 её оборота завиты влево, окрашена в желто-коричневые или бурые цвета. Нога улитки черно-синяя. Глаза расположены у основания, на внутренней стороне длинных, щетинообразных щупалец. Как и большинство других моллюсков, всеядна, хорошо очищает аквариум от остатков пищи и зеленого налета на стенках. Правда, стекла чистить все равно придется. Благоприятная температура для данных улиток должна быть не ниже 20 °С. В остальном эти моллюски нетребовательны к условиям содержания [4].

Исследование проводилось в лабораторных условиях. Использовались три аквариума, куда добавлялись концентрации нефти 1, 4 мл/л и контроль. В каждом находилось по 7 особей. Питанием служили

зеленые водоросли. Опытные исследования, проводились в течении 12 дней, в ходе которых наблюдались изменения в численности особей и изменения в поведении: двигательная активность, место нахождение, движение усиков, питание.

На 30-ой минуте после добавления нефти наблюдалось снижение двигательной активности при 1 мл/л. При 4 мл/л повышалась двигательная активность. После 24-х часов при концентрации нефти равной 1 мл/л все улитки находились на дне без признаков движения, при концентрации нефти – 4 мл/л половина улиток на дне, половина в движении. На 3-й день при концентрации нефти 1 мл/л у части моллюсков снова появилась двигательная активность. На 6-е сутки все улитки находились в движении, они располагались на стенках аквариума, в верхних слоях воды, на водорослях. Гибель части особей наблюдалась: при концентрации нефти равной 1 мл/л на 8-й день, при концентрации нефти 4 мл/л на 8-й и 10-й день.

Изменение численности моллюсков при различной концентрации нефти

День	Концентрации нефти		
	1 мл/л	4 мл/л	0 мл/л (контроль)
1-й	7	7	7
2-й	7	7	7
3-й	7	7	7
4-й	7	7	7
5-й	7	7	7
6-й	7	7	7
7-й	7	7	7
8-й	6	6	7
9-й	6	6	7
10-й	6	4	7
11-й	6	4	7
12-й	6	4	7

На основании данной таблицы построен график динамики численности особей.

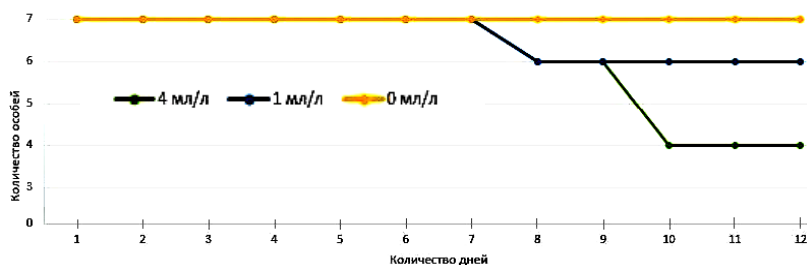


Рис. 1. Изменение численности моллюсков при нефтезагрязнениях

Таким образом на основании проведенных исследований можно сделать следующие выводы.

Выводы. В сравнении с контрольной группой загрязненных нефтью аквариумах наблюдалась смертность моллюсков, которая наступала на восьмой и десятый день наблюдения.

При концентрации нефтесмеси равной 4 мл/л количество погибших особей больше, чем при 1 мл/л.

Наблюдались изменения в поведении моллюсков

ЛИТЕРАТУРА

1. Карташев А.Г. Экологические аспекты нефтедобывающей отрасли Западной Сибири. – Томск, ТУСУР, 2007. – 218 с.
2. Карташев А.Г. Адаптация животных к хроническим факторам // LAP LAMBERT Academic Publishing, Saarbrücken, 2014. – 260 с.
3. Бедова П.В., Колупаев Б.И. Использование моллюсков в биологическом мониторинге состояния водоемов // Экология. – 1998. – № 5.
4. Улитка Физа (Physa). [Электронный ресурс]. – Режим доступа: URL: <http://oformi-akvarium.ru/mollyuski/ulitka-fiza-physa> (дата обращения: 26.02.2018).

СЕКЦИЯ 8

POSTGRADUATE AND MASTER STUDENTS' RESEARCH IN ELECTRONICS AND CONTROL SYSTEMS

(секция на английском языке)

СЕКЦИЯ 8

POSTGRADUATE AND MASTER STUDENTS' RESEARCH IN ELECTRONICS AND CONTROL SYSTEMS

(секция на английском языке)

*Председатель секции – Покровская Е.М., зав. каф. ИЯ, доцент,
к.филос.н.;*

*зам. председателя – Шнит Е.И., ст. преподаватель каф. ИЯ;
Соболевская О.В., ст. преподаватель каф. ИЯ*

SAFETY OF WEARABLE TECHNOLOGY

J. Carretero, M. Sargynbayeva, graduate students of Telecommunications and Basic Principles of Radio Engineering Department

Scientific adviser Evgeniy Rogozhnikov, Associate Professor, Ph. D.

Tomsk, TUSUR, sargosha_bookworm@mail.ru

The target of this work is to study wearable technology and issues related to the protection of information in wearable technology.

Wearable technology is a blanket term for electronics that can be worn on the body, either as an accessory or as a part of material used in clothing. There are many types of wearable technology but some of the most popular devices are activity trackers and smartwatches. One of the major features of wearable technology is its ability to connect to the Internet, enabling data to be exchanged between a network and the device. This ability to both send and receive data has pushed wearable technology to the forefront of the Internet of Things (IoT) [1].

The growing popularity of mobile networks has been one of the most important factors in the development of wearable technology. Bluetooth headsets, smartwatches and web-enabled glasses allow people to access data hands-free from Wi-Fi networks. An entire industry devoted to the development of applications that can work with wearable technologies are rapidly developing and has caught on with a trend where people began seeking new personal insights through real time data collection – often expressed as big data analytics for yourself or the quantified self. Activity trackers represented the first big wave of wearable technology to catch on with the help of social sharing. Then, as the wrist became a new screen with smartwatches, pushing notifications and adding more robust tracking

functions and processing power came naturally. Below is a table of existing wearable devices and applications for them.

Where is the technology worn?

Anatomy	Device Examples	Application Examples
Head	Cap, eye, glasses, ears	Monitor fatigue, portable computer
Neck	Necklace, chain, tie	Smartphone control, camera
Torso	Shirt, jacket, band	Monitor health, posture
Waist	Belt, fob	Monitor activity, identification and location
Upper arm	Band	Monitor activity, enhance lifting strength
Lower arm/wrist	Band, watch	Monitor fitness activity, interact with smartphone, portable computer
Hand	Ring, glove	Unlock doors, connect people, interact with touch screens in winter, SIRI/Google Now enabled
Upper thigh	Band, pants	'Smart jeans' enable smartphone interaction, enhance physical strength
Lower leg	Socks, band	Pressure sensors monitor foot injury, posture
Foot	Socks, shoes	Navigation, fitness

The Internet of Things (IoT) is heavily affecting our daily lives in many areas, ranging from tiny wearable devices to large industrial systems. Consequently, a wide variety of IoT applications have been developed and deployed using different IoT frameworks. An IoT framework is a set of guiding rules, protocols, and standards which simplify the implementation of IoT applications. The success of these applications mainly depends on the ecosystem characteristics of the IoT framework, with the emphasis on the security mechanisms employed in it, where issues related to security and privacy are pivotal [2]. There are certain frameworks to provide security of the basic infrastructure of IoT. Each framework has its own architecture, which allows you to develop third-party smart apps, the compatible hardware, and the security features. Comparison of these security architectures shows that the same standards are used to provide communication, but different methods are used to provide other security properties.

Although security is obviously important for all information systems, in the case of portable devices, the nature of the security problem is quite different and requires special attention. First, wearable machines are, of course, the most personal computing devices. They are close and personal, intimate devices that match the anatomy of a particular user. These devices control, monitor and in many cases optimize tasks perfectly and only for this person. They become part of anatomy, as in the case of diabetic contact lenses or robotic arms, which provide the wearer with a much higher lifting force. Secondly, device developers are trying to make a more attractive

design for customers, decorating their designs with precious stones and gold. Because of this, users become bait for thieves. Third, wearable devices are the first category of IT devices, where there is not only a danger for data, but also a real potential to cause physical harm to the user. Hacking a personal computer or laptop or smartphone can allow an attacker to steal data or somehow interfere with the functioning of the device. However, it is unlikely that this can lead to bodily harm to the owner. An offensive or malicious hacking of a wearable device can have consequences that can range from vexatious to heavy. Smart watches can be programmed to radiate a series of annoying, but meaningless pulses, for no reason. Breaking a diabetic's smart contact lenses to give erroneous indications can make a person either not receive warning signals or overreact to exaggerated glucose readings. This can not only have serious consequences, but can also be fatal [3].

The ultimate goal of wearable technologies is to facilitate the execution of everyday tasks, make them more efficient or simply fun. All these wearable technologies every day invade every aspect of our lives – technologies that continuously collect and process an incredible amount of data. In this context, the safety of wearable technology must be given particular attention.

REFERENCES

1. Wearable Technology [Electronic resource]. – Access: <https://www.investopedia.com/terms/w/wearable-technology.asp>
2. Ammar M., Russello G., Crispo B. Internet of Things: A survey on the security of IoT frameworks // Journal of Information Security and Applications. – 2018. – Vol. 38. – P. 8–27.
3. Mills A.J., Watson R.T., Pitt L., Kietzmann J. Wearing safe: Physical and informational security in the age of the wearable device // Business Horizons. – 2016. – Vol. 59(6). – P. 615–622.

AUTOMATED INFORMATION MANAGEMENT SYSTEM FOR PLANNING MANAGEMENT DECISIONS ON THE EXAMPLE OF SNOW REMOVAL

***T.E. Grigorieva, postgraduate student of the Department Of Computer
Control And Design Systems***

*Scientific adviser V.M. Dmitriev, DScTech, professor of the Department
Of Computer Control And Design Systems
Tomsk, TUSUR, tanya_grig_1991@mail.ru*

The problem of snow removal becomes topical with the beginning of cold weather because of climate features and geographical location of Russia, and Siberia in particular. For the last few years, the average annual

precipitation has increased in the Tomsk region and therefore the need for high quality and rational planning and organization of snow removal has increased. The automated information management system (AIMS) will provide an opportunity to improve this process.

In the article, the AIMS is understood as the system including:

- collection of information;
- complex processing of operational information (for example, about precipitation depth, traffic jams, etc.) and legislative and standard information (for example, a database of the road conditions, a database of standards and rules for organizing snow removal, etc.)
- transfer of information in the form of the necessary instructions by the management or heads of the departments to the employees of the enterprise to eliminate the current situation [1].

In the automatic mode, the system is able to perform the tasks of collecting, storing, transferring, processing and issuing information. This information is necessary for ensuring the operation of the enterprise, automating the processes of supporting management decision making, communicating the adopted decisions to the subordinates and controlling their execution and interacting with governing boards.

Thus, according to the selected object of the study, the AIMS has the following tasks for the effective management decision making:

- to identify problem areas of road networks;
- to predict the course of adopting management decisions based on the simulation model;
- to form a sequence of management decisions;
- to use management decisions in practice;
- to analyze the effectiveness of management decisions.

The structural-functional diagram of the AIMS for planning management decisions is represented in Fig. 1.

The users of this scheme can be:

- engineering-technological service, who provide the day-to-day supervision, regulation and control over the quality of snow removal;
- top management, who are responsible for making any management decision on snow removal;
- planning department, who are responsible for the process of predicting, developing and establishing a system of the quantitative and qualitative indicators at the enterprise and who facilitate the selection of the most optimum ways to achieve the objectives of the enterprise;
- production control department, who are engaged in developing the regulatory information, as well as forming the routing and scheduled maintenance task cards for snow removal, etc.

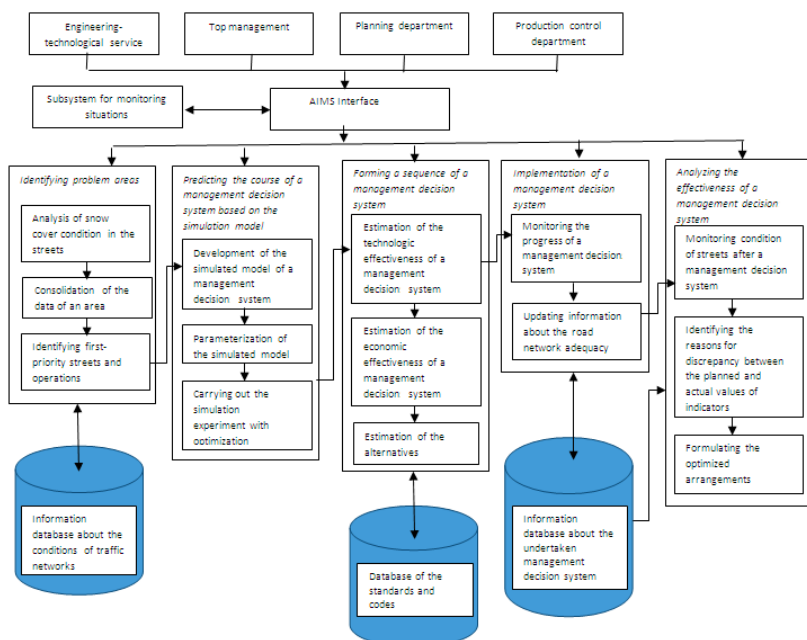


Fig. 1. The structural-functional diagram of the AIMS for planning management decisions

We will consider the structure of the AIMS in more detail.

To identify the problem areas of a town, there exists the analysis of snow cover condition in the town streets. It is based on real time data from the Weather Service and data about road conditions. Then, we identify the first-priority streets for snow removal according to the classification of roads [2]. As a rule, these are the principal traffic roads of the town and the streets for public transport.

To predict the management decisions, we develop a simulation model of snow removal. The parameterization of the simulated model is carried out by GISMETEO and 2GIS API. API is a programming interface of an application for the interaction between the site and the simulation model. After the model parameterization is done, we conduct an experiment taking into account optimization of the resources available.

The parameters of technologic (the optimum quantity of required custom vehicles, timetable, etc.) and economic (the costs associated with snow removal) effectiveness are estimated at the end of the experiment. Based on the estimates of the required parameters, the advantages and disadvantages of the decision options are determined, and the best alternative is chosen,

i.e. the decision that is most suitable for solving the given problem when using the least amount of resources [3].

The implementation of management decisions takes place after the formation of their sequence. It allows defining correctness and optimality of the decision made, monitoring and updating information about adequacy of the road networks.

At the end of planning a management decision, we make the analysis of its effectiveness, which is provided by identifying the reasons for discrepancy between the planned and actual values of indicators, after which, if necessary, the optimized arrangements are formed.

In conclusion, it should be noted that the AIMS for planning management decisions on the example of snow removal in an automated fashion gives a possibility to predict the course of creating management decisions based on the simulation model, and to analyze their effectiveness, considering conditions of the road networks and the existing standards, as well as the rules for cleaning streets.

REFERENCES

1. P'javchenko T.A. Finaev V.I. Avtomatizirovannye informacionno-upravljajushhie sistemy [Automated information management systems]. – Taganrog: Izd-vo TRTU, 2007. – 271 p. (in Russian).
2. GOST 33181–2014 «Dorogi avtomobil'nye obshhego pol'zovanija. Trebovanija k urovnju zimnego soderzhanija» [Public roadways. Requirements for the level of winter maintenance/] – Available at: <http://www.internet-law.ru/gosts/gost/60919/> (accessed 01.02.2018) (in Russian).
3. Dorofeev L.I. Osnovy teorii upravlenija [Fundamentals of control theory]. – Saratov, 2015. – 433 p. (in Russian).

ELECTRODYNAMIC SIMULATION OF THE ULTRASHORT PULSE DECOMPOSITION IN THE SEVEN-STAGE MODAL FILTERS LAYOUTS

R.R. Khazhibekov, Master's program student

Head of research A.M. Zabolotsky, professor of Television and Control dep., Ph.D.

Tomsk, TUSUR, r300994@mail.ru

Today, Ethernet 100Base-T (Fast Ethernet) technology is widely used for data transmission in different types of networks. The problem of protection against intentional electromagnetic interference is very important. Therefore, it is urgent to develop devices protecting network equipment from such interference. Surge arresters, varistors, TVS-diodes or galvanic transformer isolation are commonly used to protect equipment from con-

ductive interference. There has also been a proposal to use modal filters (MFs) for this purpose, as they contain no radioelectronic components, and have special structures used to facilitate the decomposition of dangerous high-voltage ultrashort pulses (USPs) and smaller pulses of up to several hundred picoseconds. The MF has a long service life, uses cheap material and is resistant to radiation [1].

The first construction of the seven-stage MF4 was presented in [2]. Later, an improved construction with the aligned width of half-turns was developed [3]. It is necessary to evaluate the effectiveness of protection against USPs for these structures. The purpose of this work is to perform electrodynamic simulation of the response to USPs in the printed circuit boards of the seven-stage MFs.

The investigated structures are shown in Fig. 1. The MF conductors have the following dimensions: width is 0.3 mm, height is 0.105 mm and length is 1300 mm. The passive and reference conductors are interconnected by the openings passing through the dielectric substrate. The conductor material is copper; the substrate is FR-4.

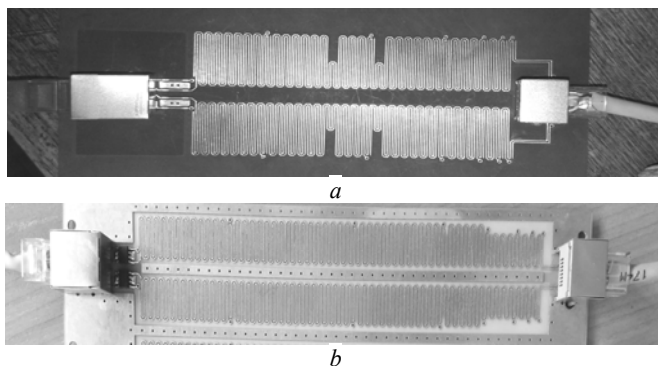


Fig. 1. MF4 (a) and improved MF4 (b)

The MF connection diagram is shown in Fig. 2. Resistance values are $R_1=R_2=R_3=R_4=50\text{ Ohm}$. A USP with an amplitude of 10 V and duration of 0.3 ns (Fig. 3) is applied to the input of the active conductor.

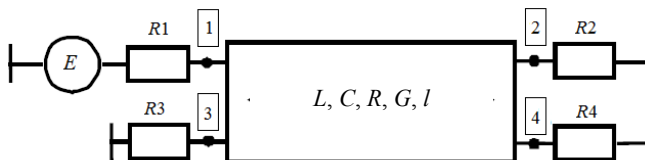


Fig. 2. MF connection diagram

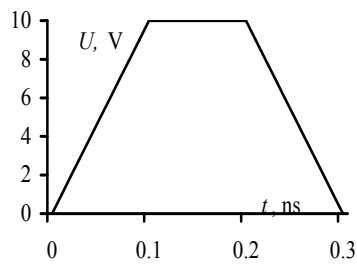


Fig. 3. Input USP

Figure 4 shows the response to the USP at the output of the MFs, which was obtained by electrodynamic simulation.

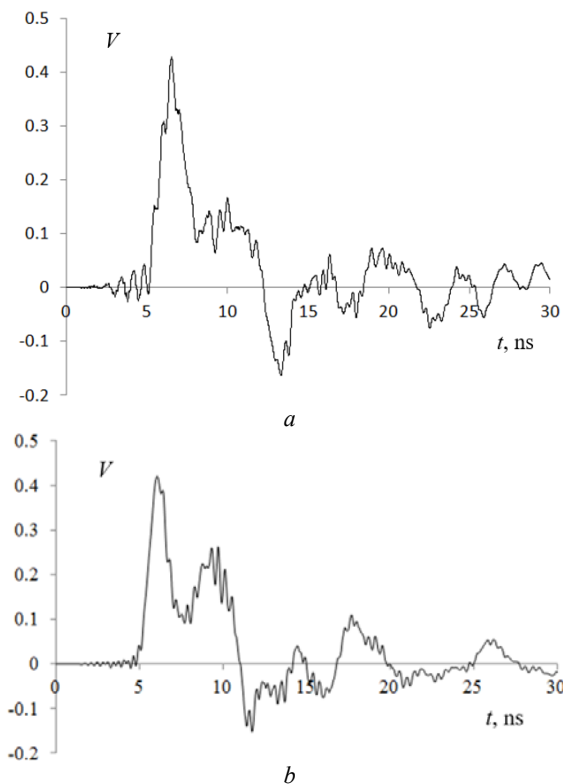


Fig. 4. Response to USP at the output of MF4 (a) and improved MF4 (b)

The maximum output voltage of the MF4 is 0.43 V and the voltage at the output of the improved MF4 is 0.42 V. Thus, the presented MFs effectively protect Ethernet equipment from USPs.

This research was supported by the Russian Federation President grant №14.256.18.356-MD.

REFERENCES

1. Kuksenko S.P., Khazhibekov R.R., Gazizov T.T. Estimation of radiated electromagnetic emission level from seven-stage modal filter for Ethernet 100Base-T network // Technology of electromagnetic compatibility. – 2017. – No 1(60). – P. 13–20 (in Russian).
2. Samotin I.E. Devices for protecting computer facilities and control systems by modal decomposition of interference pulses in cable and strip structures: PhD thesis. – 2011. – 199 P. (in Russian).
3. Kropotov V.V. Research and development of a twelve-channel device for protecting Ethernet equipment from conductive interference: Master's dissertation. – 2017. – 82 P. (in Russian).

STATIC RECIPROCAL CONVERTER

*V.V. Ignatenko, postgraduate student, Department
of Industrial Electronics;*

*O.V. Bubnov, Head of the 14th Department of Scientific and Research
Institute of Automatics and Electromechanics, PhD*

*Scientific supervisor A.G. Yudintsev, Head of the 13th Department of Scientific and Research Institute of Automatics and Electromechanics, PhD
Tomsk, TUSUR, ignatenko.vlas@gmail.ru*

The power conditioning unit (PCU) of the spacecraft is one of the essential systems providing the trouble-proof functioning of the satellite in orbit. [1] Connection of onboard primary energy sources (solar and storage batteries) and satellite-borne equipment during ground tests is difficult. The main reasons are the lack of the solar energy equal to the energy in the outer space, the inability to set the required operating point on the current-voltage curve of the solar and storage batteries, as well as the inability to connect the required load of the spacecraft to the PCU [2]/

The Scientific Research Institute of Automatics and Electromechanics (Tomsk, Russia) designs simulating complexes for companies which are engaged in the production of spacecraft. The Institute's developments are a battery simulator, a solar battery simulator, a load simulator, a charge-discharge software and hardware complex, etc. [3] The next step in the development of ground-based test complexes is the design of a universal

complex. We have developed a static reciprocal converter (SRC) (Fig. 1) to solve this problem.

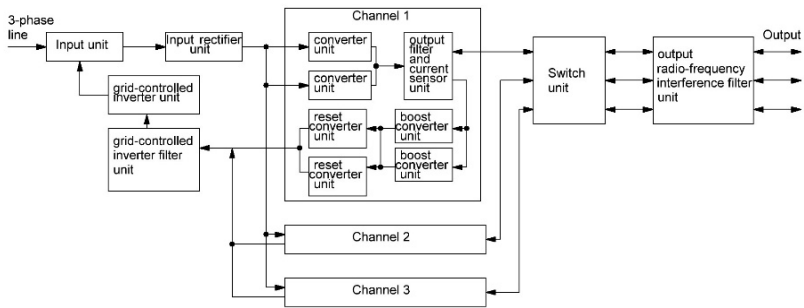


Fig. 1. Block diagram of the SRC

The SRC is designed to simulate the onboard storage batteries of the PCU in the stage of ground testing and to reduce the duration of these tests. The SRC contains three independent channels, each of which can operate in 3 different modes: a battery simulator mode (charge and discharge battery modes), a ground voltage source simulator mode and an electronic load mode. The first operation mode of the SRC channel is based on converting the AC power of the primary line to DC power and transferring it to the load during the discharge battery mode and the voltage source mode. The second operation mode is based on converting the input DC power into AC power and transferring it to the line during the charge battery mode and the electronic load mode.



Fig. 2. The main user interface window

The SRC carries out permanent hardware and software monitoring and emergency diagnostics of electronic units and switching equipment. The SRC is disconnected from the testing system when protection is triggered. In this case, the SRC is automatically turned off and blocks the power side and connection to the product. An "ALARM" banner and the cause of the accident are displayed.

The embedded SRC software provides:

- data exchange with an external computer via the Ethernet communication interface;
- SRC failure monitoring and diagnostics;
- SRC testing;
- reference setting;
- load connection control;
- user interface (Fig. 2).

Double energy conversion makes the energy recuperation into the primary line possible, so that long-time testing operates in the energy-saving mode.

REFERENCES

1. Systems of communication satellites: A manual on the course «Electric power systems of AC» / A.B. Bazilevsky, A.G. Kozlov, M.V. Lukyanenko and others. – Krasnoyarsk, 1989. – 224 p. (in Russian).
2. Yudintsev A.G. The development problems of automated control system for spacecraft's power systems//International science conference «Reshetnevskie chteniya». – Krasnoyarsk, 2013. – Part 1. – P. 336–337. (in Russian).
3. Yudintsev A. G., The automated power saving hardware of constant current load emulator//International science conference «Reshetnevskie chteniya». – Krasnoyarsk, 2014. – Part 1. – P. 335–336. (in Russian).

MACHINE VISION OF THE INMOOV ROBOT

Z.M. Kurmasheva, graduate student of the IE Dept;

A.S. Fedurin, student of the ISS Dept;

F. Videau, student of the CISCS Dept

Scientific supervisor Yu.O. Loboda, Associate Professor,

PhD in Engineering Science, the CISCS Dept

Tomsk, TUSUR, yulloboada@gmail.com

InMoov is a first life-size humanoid robot, which can be 3D printed and animated. InMoov robot can be used as an initial step in universities and laboratories. InMoov was created using the Blender software and launched using the MyRobotLab program, which is publicly available. An important part of creating a robot is the choice of a machine vision system.

A facial recognition system is a computer application capable of identifying or verifying a person from a digital image or a video frame from a video source [1]. The use of computer technology for face recognition dates back to 1960s. The men who first worked on it was called Woodrow Wilson Bledsoe. At that time the major points and coordinates on the face had to be set by hand. This made the face recognition difficult, long, and not precise and all of it was caused by the limitations of the technology. The first improvement was made by Jay Goldstein, Leon Harmon and Ann Lesk in the 1970s. They added more mark points on the face to increase the precision. The problem with this method was that, like Bledsoe method, the points had still to be entered manually [3]. For the InMoov robot we chose the Fisherface algorithm, since it demonstrates the best results from the experimental data when analyzing images with different lighting.

Despite a wide range of algorithms, it is possible to distinguish the general structure of the facial recognition process. Fig. 1

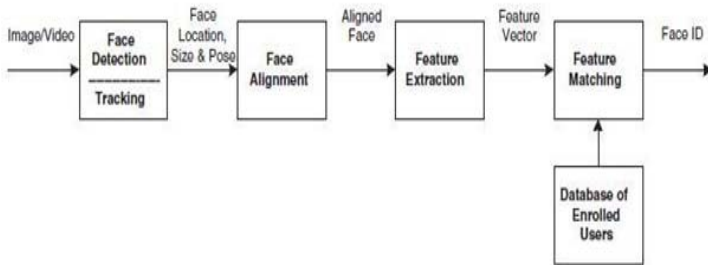


Fig. 1 Face recognition processing flow

At the first stage, the face is detected and localized in the image. At the recognition stage, the image is aligned (geometry and light). For the ability to recognize faces, we used the Fisherface algorithm. The Fisherface method of face recognition uses both principal component analysis and linear discriminant analysis to produce a subspace projection matrix. However, the Fisherface method is able to take advantage of intraclass information, minimizing variation within each class, yet still maximizing class separation [2].

As mentioned earlier, the selection of the machine vision system is an integral part in creating a robot. In this study, cameras were selected for the robot's head and for its abdominal cavity. Installing cameras in the head of the robot, specifically in the eyes, is conditioned by the need to subsequently make it possible for the robot to recognize faces. The camera in the abdominal cavity of the robot will perform the function of orienting in space. Installation of this camera is caused by the need to avoid obstacles when moving in the area.

Machine vision (MV) is the technology and methods used to provide imaging-based automatic inspection and analysis for such applications as automatic inspection, process control, and robot guidance, usually in industry. The first step in the automatic inspection sequence is the acquisition of an image, typically using cameras, lenses, and lighting, that has been designed to provide the differentiation required by subsequent processing. MV software packages and programs developed in them then use various digital image processing techniques to extract the required information, and often make decisions (such as pass / fail) based on the extracted information [4]. Machine vision commonly provides location and orientation information to a robot. This capability is used to guide motion that is simpler than robots, such as a 1 or 2 axis motion controller. The overall process includes planning the details of the requirements and project, and then creating a solution [5]. At the core of the vision system is a digital camera that removes the surrounding space, then the resulting data is processed by the processor using the algorithm, in this case the Fisherface algorithm. At this stage, the data is prepared and output in a form suitable to be processed by the robot controller. The data is then transferred directly to the robot controller, where we can use it to control the robot. In the work done at TUSUR we carried out the research into the different types of «vision», which can be used in the face recognition system of the InMoov robot. We explored and compared different types of cameras. The results of this part of research are presented in Table. For the head of the InMoov robot, we chose the Microsoft LifeCam 3000 HD camera, the main characteristics of which are: type of matrix is CCD, number of megapixels is 1,3 MP, video resolution is 1280x720, maximal frame rate is 30 fps.

Comparing different types of cameras

	1 standard camera	2 standard cameras	Infrared camera	3d scanner	Sonar
Usable at night	No	No	Yes	Yes	Yes
2D/3D	2D	3D	3D	3D	3D
Detects colors	Yes	Yes	No	Not at night	No
Works under the water	Not good	Not good	Not good	No	Yes
Works through glass	Yes	Yes	Not good	No	No
Element used	Light	Light	Infrared radiation	Lasers	Sound
Responsivity	Good	Good	Medium	Good	Medium

For the robot body we chose the Intel RealSense Developer Kit. Intel RealSense is a camera with three modules: a conventional camera with a

resolution of 1080p, an infrared camera and an infrared laser projector. The device with an Intel RealSense camera called RealSense Robotic Development Kit consists of a small single-board computer and a RealSense R200 camera. It has Atom x5-Z8350 processor, 4 GB of RAM, 32 GB of eMMC flash memory, a real-time clock (RTC), one USB 3.0 port, four USB 2.0 ports, and Gigabit Ethernet, HDMI 1.4b, CSI and 40 pin connector.

REFERENCES

1. Facial recognition system [Electronic source]. – URL: https://en.wikipedia.org/wiki/Facial_recognition_system (date of the application: 19.02.2018).
2. Comparison between face recognition algorithm-eigenfaces, fisherfaces and elastic bunch graph matching [Electronic source]. – URL: <http://www.jgrcs.info/index.php/jgrcs/article/viewFile/46/46> (date of the application: 02.02.2018).
3. Face Biometrics. Introduction and History [Electronic source]. – URL: <https://www.jadelearning.com/jadecc/courses/UNIVERSAL/NEC05.php?imDif=6489.0> (date of the application: 21.01.2018).
4. Machine vision [Electronic source]. – URL: https://en.wikipedia.org/wiki/Machine_vision (date of the application: 19.02.2018).

THE STUDIES OF THE MINERAL COMPOSITION OF NATURAL WATERS OF SIBERIA RESORTS

A.A. Leshenok, student, O.A. Lisuro, student,

Supervisors: M.V. Plankina, T.A. Belomestnykh – teachers,

Tomsk Industrial Humanitarian College

Tomsk, Industrial Humanitarian College, kirpl57@mail.ru

In Siberia, there are many different curative natural resources used for resorts and rest homes. Therefore, any of the diseases that are usually treated at the resorts of the south and the European part of the CIS, as well as at famous resorts of Western Europe, can receive no less successful treatment at local health resorts.

The purpose of this work is:

1. to determine the chemical composition of waters in reservoirs and mineral springs sources at the resorts of Siberia;
2. to compare the obtained experimental data with each other, and further with the waters of the famous resorts.

The famous sanatoria-resorts of the Siberian region are Belokurikha, Karachi, Chazhemto, and Shira. The advantage of these resorts is mineral water. The presence of various ions in water is of great importance for its therapeutic and biological effect. In mineral waters there, up to 50 different

chemical elements were found. However, the main ions that determine the curative properties of waters are: Na^+ , K^+ , Cl^- , Mg^{2+} , Cl^- , SO_4^{2-} , HCO_3^- [1].

The listed ions make up from 90 to 95% of the total amount of dissolved substances in the waters. In addition, ammonia and nitrates are present in the water, which impairs the properties of water. Water samples were analyzed for the content of microelements. The water analysis was carried out for three samples of each type of water, using methods denoted in [2]. The determination of potassium and sodium was carried out by flame photometry on a flame photometer of PFM. The determination of Ca^{2+} and Mg^{2+} ions was carried out by complexometric titration with a solution of Trilon B. The determination of chlorides, sulfates, nitrates and ammonia was carried out photocolrimetrically on KFK-3. The experimental data of the analyzed waters are presented in Table 1.

As a result, we see that the water of Lake Karachi is close to the water of Lake Tus from Khakassia in chemical composition. However, more magnesium cations and chlorine ions are observed in Lake Karachi.

The water of Lake Shira is of a sulphate-chloride-magnesium type; the water of Lake Itkul and Lake Fyrkal is of a hydrocarbonate-sulphate-magnesium type. The water of Lake Karasevoye is chemically hydrocarbonate-chloride water and, in comparison with the waters of Lakes Shira and Karachi, it is less mineralized and practically does not contain magnesium cations.

Table 1

The content of macroelements in lakes

The Ions The lakes	F_{total} mmol/l	Ca^{2+} mg/l	Mg^{2+} mg/l	HCO_3^- mg/l	Cl^- mg/l	SO_4^{2-} mg/l	NH_4^+ mg/l	NO_3^- mg/l	Dry residue g/l
Lake Shira	330,0	100,0	3900,0	700,0	2100,0	7200,0	0,7	2,0	21,9
Lake Tus	760,0	600,0	8760,0	1855,0	39500,0	4700,0	0,4	1,6	236,0
Lake Itkul	6,0	28,0	55,2	400,0	17,5	67,5	0,4	0,8	0,8
Lake Fyrkal	4,0	16,0	38,4	300,0	1,3	27,5	0,7	1,2	0,7
Lake Karasevoye	4,6	80,0	7,8	203,7	1700,0	32,0	0,7	1,6	5,6
Lake Karachi	1320,0	1000,0	15240,0	1220,0	62500,0	6400,0	0,8	1,2	208,7
The Dead Sea	5183,7	16860,0	45345,0	220,0	227545,0	470,0	-	-	350,5
Lake Baikal	1,0	15,2	3,1	66,5	0,5	5,2	n/o	n/o	60,0
MAC	7,0	180,0	40,0	-	300,0	100,0	0,5	40,0	1000,0

Taking into account the classification of the waters according to their total mineralization and based on the tabulated data, the waters of Lakes Itkul and Fyrkal can be classified as low mineralization waters, the Shira

water as high mineralization water, the waters of Lakes Tus and Karachi as brines.

For comparison, Table 1 includes the values of the total mineralization of the Dead Sea water – the world's famous salt lake, the largest natural mineral source on earth. The waters of Lakes Tus and Karachi are only slightly inferior to the Dead Sea as regards total mineralization.

As it can be seen from the table, the purest water in terms of the content of impurities is in Lake Baikal, in which there is no excess of the maximum admissible concentrations of impurities in any of the indices. Also, of all the lakes we have analyzed, Itkul and Fyrkal are the purest in terms of the content of macroelements.

The increased content of nitrates and ammonia in the waters of lakes is an indicator of household pollution and is associated with microbiological processes, human activities, and sanitary conditions.

Table 2 shows the most significant mineral waters and wells. Based on the obtained data, it can be concluded that the water of the well of the Chazhemto resort has the macroelemental composition of a hydrocarbonate-chloride-sodium type.

The mineral water from the well of the resort of Karachi is similar to the water of Yessentuki in composition and medicinal properties: it has a chloride-hydrocarbonate-sodium composition. Also, they are close in terms of the content of potassium and sodium. Consequently, it is now more convenient and profitable for Siberians to travel to the Siberian resort of Karachi. In addition to the mineral water, there is a unique lake with high mineralization water, similar to the water of Lake Tus and the Dead Sea.

Table 2

The content of macroelements in mineral waters and wells

The Ions	K ⁺ mg/l	Na ⁺ mg/l	Ca ²⁺ mg/l	Mg ²⁺ mg/l	SO ₄ ²⁻ mg/l	Cl, mg/l	HCO ₃ ⁻ mg/l	Dry residue g/l
Well 8P	15,80	586,00	248,00	14,40	0,10	2950,00	231,80	4,90
Well 6P	2,20	240,00	8,00	2,40	0,20	2800,00	366,00	3,80
Well 5P	18,30	600,00	240,00	7,20	35,00	3250,00	483,00	5,20
Mineral water «Chazhemto»	1,70	253,00	4,00	1,80	0,10	640,00	433,10	1,20
«Belokurikhin- eastern» (well №2)	4,50	269,00	380,00	132,00	200,00	816,60	220,00	2,02
Dunyashin spring	1,81	39,30	44,00	9,60	н/о	н/о	219,60	0,39
Silver key	0,54	5,90	42,30	14,40	3,70	н/о	190,00	0,31
Well-Resort Karachi	18,40	650,00	38,00	40,10	95,80	484,00	870,00	2,20
Mineral water «Essentuki №4»	20,80	731,00	143,20	53,60	108,00	750,20	1272,00	4,80
The well-spa Baden- Baden	5,05	250,60	129,35	0,27	152,81	1437,60	155,10	2,90

Mineral water «Belokurikhinskaya – Vostochnaya» from the well № 2 of the resort of Belokurikha is comparable to the water of the famous resort of Baden-Baden. Similarities are observed in the content of hydrocarbons, chlorides, sulfates, sodium, and potassium. And in terms of the content of calcium and magnesium, this water exceeds the water of the resort of Baden-Baden. Therefore, the water of the resort «Belokurikha» can be recommended for the treatment of the same diseases.

The conducted researches allow us to make the following conclusions.

1. The health resorts of Western and Eastern Siberia are not only comparable to the glorified southern and European resorts, but also surpass some of them. As it was already mentioned, the water of the resort of Belokurikha is superior to the water at the resort of Baden-Baden in terms of the content of some macroelements.

2. The presence of such a variety of natural and mineral waters with different chemical compositions allows Siberians to replace well-known mineral waters with local waters and to be treated at Siberian resorts.

REFERENCES

1. Sprugin I. Mineral waters that we drink. Collection of research works of the VII All-Russian Competition of Youth Research. – Moscow: Nauka, 2000. – P. 98–99 (in Russian).
2. Vasiliev V.P. Analytical chemistry. In 2 hours Part 2. Physical and chemical methods of analysis: Proc. for chemical technology. specialist. universities. – M.: Higher education. Shk., 2004. – 384 p. (in Russian).

ELECTRICAL NETWORK MONITORING VIA THERMOELECTRICAL COMPONENTS

*I.I. Obach, postgraduate student, Department of Innovation
Management;*

*A.A. Abouellail, postgraduate student, Department of Industrial and
Medical Electronics*

*Scientific supervisor A.I. Soldatov, Professor, Department of Innovation
Management, Doctor of Engineering Sciences.
Tomsk, TUSUR, obachigor@gmail.com*

Statistics of fire outbreaks. The operation of residential, domestic, industrial and other facilities is often accompanied by fires, arising from faults in the wiring or other elements of the electrical network and electrical installations (24%). The result is great material and moral damage often exacerbated by injuries and even deaths [1].

According to the recent statistics from the Russian Ministry of Emergency Situations for 2017, a large proportion of the reasons are fires resulting from faults in electrical networks, as seen in Figure 1. These imply poor quality of installing electrical network elements and violations of their proper operation requirements.

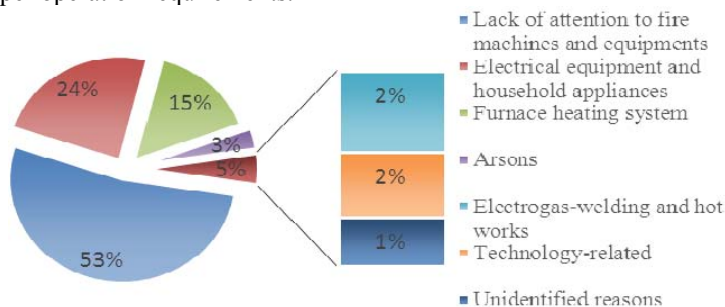


Fig. 1. Statistics of the main causes of fires

The causes of electrical fires are:

- short circuits;
- mismatching current load on sockets, cables, machines;
- overload on electrical networks;
- local overheating;
- critical contact resistance;
- leakage of electric current to grounded metal structures of buildings and structures;
- leakage of electric current to low-current electric lines (radio, telephone, etc.);
- high transient contact resistance.

In this article, we propose a method for detecting a local overheating because of the large transient contact resistance.

Transient Contact Resistance. This is the resistance of a section of an electrical circuit at the junction of individual elements (the places of connecting the wires, connecting them to electric receivers, contact elements) in which, if not correctly coupled, the resistance is higher, compared to the resistance of the electrical circuit to these sections [2].

The formation of sources of ignition in the event of large transient resistances, as a rule, is possible at places where the transient resistances described above appear. The immediate source of ignition in this case can be: elements of electrical installations heated up to a high temperature by heat emitted by an electric current at the place of a large transient resistance; electric sparks or particles of molten and heated metal that occur at the site

of a poor electric contact. This implies that it is necessary to, periodically, monitor networks for problems.

Devices for network monitoring. To date, there are alarming instruments that are based on different principles of monitoring dangerous operation of wiring.

Instrument types are the following: thermal [3, 4], current-limiting [5], total current [6], measuring instruments [7, 8].

The disadvantages of modern instruments and methods for monitoring and controlling networks have pushed us towards looking for new ways to solve this problem. For the first time, it is proposed to use the thermoelectric method for monitoring networks, which is based on the phenomenon of Seebeck.

Network monitoring device based on thermoelectric method. The task of this device is to prevent fires that occur in rooms, structures, buildings. The device belongs to the field of fire safety and electric power industry, specifically to methods and devices for preventing fires that occur due to malfunctions of electrical networks or electrical installations in rooms, structures, buildings, aircraft, ships, railway transport and other objects.

Figure 2 shows the method of employing the device for network monitoring, where its operation is based on the current flow in the circuit with the contact resistance R_{cont} . The device is connected to the input electrical lines from the electrical panel side. Poor twisting or wear of contacts at the junctions site will generate heat in accordance with the Joule-Lenz law [9] and, as a result, there will be a thermoelectric power which will indicate a problem in the wiring. If the materials used in the network are known, for the sake of clarity, the quantitative value of the thermoelectric power can be converted to degrees.

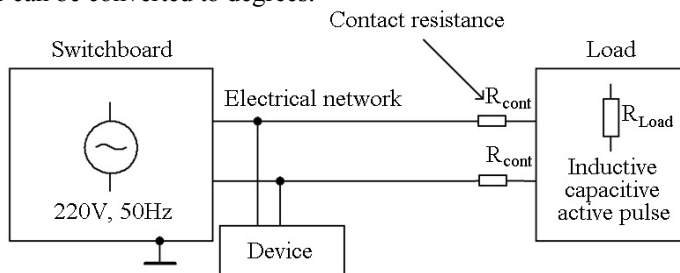


Fig. 2. Structural diagram of connecting the inspection device

The technical result is an increase in fire safety. Thus, the introduction of the proposed method of preventing fires in case of malfunctions in the electrical network or electrical installation will increase the protection of people, residences, industrial and other objects from the damaging effects

of fire accidents, and provide substantial savings to the material and financial resources of each citizen and the state as a whole.

REFERENCES

1. The website of EMERCOM of Russia data for 2017 [Electronic resource]. – URL: http://www.mchs.gov.ru/activities/stats/Pozhari/2017_god (accessed 18.12.2017).
2. Electronics. Encyclopaedic dictionary. – M.: Soviet encyclopedia, 1991. – P. 530–541, 544–545.
3. Lloyd G. Thermal imaging systems / Per. from English. under the editorship of A.I. Goryachev. – M.: Mir, 1978. – 416 p.
4. Patent of Russia RU 0001581 U1, CL. H 02 N 3/08.
5. The patent of Russia RU 2159468, C1 7 G08B 17/ 06, G08B 25/10.
6. GOST 8.366–79. State system for ensuring the uniformity of measurements. Digital ohmmeters. Methods and means of verification.
7. Blatt F.J., Schroeder P.A., Folz K.L. Greig Thermoelectric power of metals. – M., 1980. – 248 p.
8. Abouellail A., Obach I., Soldatov A. Surface inspection problems in thermoelectric testing / MATEC Web of Conferences 102, 01001.
9. Soldatov A.A., Sorokin V.P., Soldatov A.I., Abouellail A.A., Obach I.I., Bortalevich V.Y., Shinyakov Y.A., Sukhorukov M.P. An experimental setup for studying the electric characteristics of thermocouples / SIBCON 2017. – Proceedings.

THE CATALAN AND EULER NUMBER TRIANGLES AND THEIR APPLICATION

***Y.V. Shablya, PhD student, Department of Complex Information
Security of Computer Systems***

*Scientific Supervisor A.A. Shelupanov, Doctor of engineering, Professor,
Head of Department of Complex Information Security of Computer Systems
Tomsk, TUSUR University, syv@keva.tusur.ru*

A number triangle is a doubly indexed sequence in which the length of each row corresponds to the index of the row. One well-known example of a number triangle is Pascal's triangle [1], whose elements are the numbers of k -combinations of an n -set denoted as C_n^k or binomial coefficients $\binom{n}{k}$.

Pascal's triangle has a wide range of properties and finds its application in various fields of mathematics. Also, there are many other number triangles that are useful for in solving some theoretical and applied problems.

Consider Catalan's number triangle [2] (Table 1):

Table 1

Some values of Catalan's triangle

n / m	0	1	2	3	4	5	6	7	8
0	1								
1	1	1							
2	1	2	2						
3	1	3	5	5					
4	1	4	9	14	14				
5	1	5	14	28	42	42			
6	1	6	20	48	90	132	132		
7	1	7	27	75	165	297	429	429	
8	1	8	35	110	275	572	1001	1430	1430

The elements of Catalan's triangle have a whole set of combinatorial interpretations. One of the earliest historically formed interpretations is ballot numbers [3]. For example, if there are n votes for the first candidate and $m \leq n$ votes for the second candidate, then the ballot numbers show the number of ways to count votes sequentially so that at any time during the counting the majority of votes for the second candidate is not shown.

Catalan's triangle is given by the following formulas:

– an explicit formula:

$$C_{n,m} = \frac{n+1-m}{n+1} \binom{n+m}{m} = \binom{n+m}{m} - \binom{n+m}{m-1};$$

– a recurrence formula:

$$C_{n,m} = \begin{cases} 1 & \text{for } m = 0, \\ C_{n,m-1} & \text{for } m = n, \\ C_{n,m-1} + C_{n-1,m} & \text{otherwise;} \end{cases}$$

– an ordinary generating function:

$$C(x, y) = \sum_{n=0}^{\infty} C_{n,m} x^n y^m = \frac{C(x \cdot y)}{1 - x \cdot C(x \cdot y)},$$

where $C(x) = \frac{1 - \sqrt{1-4x}}{2x} = \sum_{n=0}^{\infty} C_n x^n$ is an ordinary generating function for

the sequence of the Catalan numbers C_n [4].

Consider Euler's number triangle [1] (Table 2):

The elements of Euler's triangle are the Eulerian numbers [1], a combinatorial interpretation of which is the number of permutations of n elements with k ascents. That is, the number of permutations of numbers from 1 to n in which exactly m elements are greater than the previous element.

Table 2

Some values of Euler's triangle

n / m	0	1	2	3	4	5	6	7	8
0	1								
1	1	0							
2	1	1	0						
3	1	4	1	0					
4	1	11	11	1	0				
5	1	26	66	26	1	0			
6	1	57	302	302	57	1	0		
7	1	120	1191	2416	1191	120	1	0	
8	1	247	4293	15619	15619	4293	247	1	0

Euler's triangle is given by the following formulas:

– an explicit formula:

$$E_{n,m} = \sum_{k=0}^{m+1} (-1)^k (m+1-k)^n \binom{n+1}{k};$$

– a recurrence formula:

$$E_{n,m} = \begin{cases} 1 & \text{for } m = 0, \\ 0 & \text{for } m = n, \\ (n-m) \cdot E_{n-1,m-1} + (m+1) \cdot E_{n-1,m} & \text{otherwise;} \end{cases}$$

– an exponential generating function:

$$E(x, y) = \sum_{n=0}^{\infty} \frac{E_{n,m}}{n!} x^n y^m = \frac{y-1}{y - e^{x(y-1)}}.$$

On the basis of Catalan's and Euler's triangles, we can construct another number triangle; for example, consider a number triangle of the following form (Table 3):

Table 3

Some values of Euler-Catalan's triangle

n / m	0	1	2	3	4	5	6	7	8
0	1								
1	0	1							
2	0	1	1						
3	0	2	3	1					
4	0	5	8	7	1				
5	0	14	23	26	15	1			
6	0	42	70	89	80	31	1		
7	0	132	222	302	335	242	63	1	
8	0	429	726	1032	1294	1265	728	127	1

An explicit formula of the presented triangle:

$$EC_{n,m} = \begin{cases} 1 & \text{for } m = n, \\ \sum_{k=0}^m E_{m,k} \cdot C_{n-1,n-m-k} & \text{otherwise.} \end{cases}$$

An exponential generating function:

$$EC(x, y) = \sum_{n=0}^{\infty} \frac{EC_{n,m}}{m!} x^n y^m = \frac{1}{1 + C(x) \cdot (e^{x \cdot y} - 1)}.$$

Thus, the study of number triangles has not only theoretical importance but also practical applicability, because it is possible to define a combinatorial interpretation that will find its application in practice.

This work was partially supported by the Ministry of Education and Science of Russia, Government Order no. 2.8172.2017/8.9 (TUSUR).

REFERENCES

1. Graham R.L., Knuth D.E., Patashnik O. Concrete mathematics. – Addison-Wesley, 1994. – 657 p.
2. Bailey D.F. Counting arrangements of 1's and -1's // Mathematical Magazine. – 1996. – №69. – P. 128–131.
3. Zatorskii R.A., Malyarchuk A.R. Generalization of the ballot numbers // Mathematical Notes. – 2011. – №90 (4). – P. 527–529.
4. Stanley R.P. Catalan Numbers. – Cambridge University Press, 2015. – 222 p.

ANALYSIS OF THE DEPENDENCE OF LOSSES ON THE GAP WIDTH BETWEEN WAVEGUIDES OF THE SPOT-SIZE CONVERTER

R.Yu. Shageev, graduate student, department of Physical Electronics
Research supervisor I.V. Kulinich, engineer of Nanotechnology Research and Education Center
 Tomsk, TUSUR, shageevr@gmail.com

Generally, in optics the spot-size converter is a waveguide, the dimensions of which vary, and this causes the change of the light beam size. Such device is used in integrated optics for reduction of optical losses [1]. One of the implementations of the spot-size converter is a light splitter.

This paper presents an analysis of geometry of the spot-size converter and the dependence of losses in waveguides on the gap width between them.

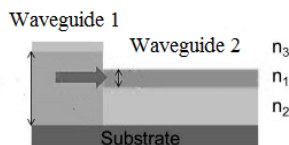


Fig. 1. Spot-size converter

Figure 1 shows a schematic image of the spot-size converter. Due to this design, it is possible to control the size of the light beam and the direction of light propagation.

To study the dependence of losses in waveguides on the gap width between them, the spot-size converter was modeled as a light splitter. For our simulation, we used COMSOL Multiphysics® software for multi-physical modeling.

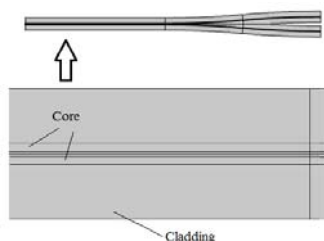


Fig. 2. Spot-size converter as a light splitter

The losses measurement was carried out at zero bias and we only took into account the geometry of the device.

The parameters specified in the modeling are given in Table.

Spot-size converter parameters

Parameter		Value
Wavelength		1550 nm
Refractive index		GaAs/AlGaAs
	core	3.43
	cladding	3.38
Electro-optic coefficient		1.5 pm/V
Relative permittivity		12

After the model was built, we changed the gap width between the waveguides and measured the losses. The dependence of losses on the gap width between waveguides in the light splitter is shown in Figure 3.

As we can see, an increase of the gap width causes electromagnetic losses in the spot-size converter. There is a critical magnitude of the gap width at which the wave splits exactly in half. A further decrease of this magnitude also leads to the increase of losses.

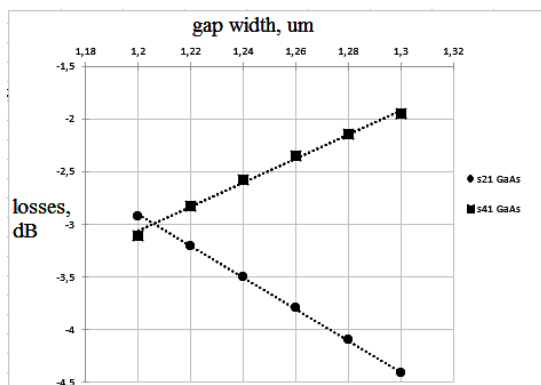


Fig 3. Dependence of losses on the gap width between waveguides in the GaAs light splitter

This study looks promising for building the spot-size converter geometry and further development of the integrated light splitter.

REFERENCES

1. Karnaushkin P.V., Ponomarev R.S. The optical fiber with a taper lens to light input into the waveguide of a small diameter // Bulletin of Perm University. – Physics. – 2017, no. 1 (35). – P. 54–63.

HYBRID VEHICLE FOR FULL AUTONOMY

A. Zalevskii, R. Vaissie, graduate students of Telecommunications and Basic Principles of Radio Engineering Dept.

Scientific adviser Evgeniy Rogozhnikov, Associate Professor, Ph.D. Russia, Tomsk, TUSUR, nhbx@mail.ru

Problem. People with limited mobility have many problems associated with moving around in the house and outside. Today about 2% of the world's population are in wheelchairs. A wheelchair is a technical assistance to mobility that allows transporting a person. However, just movement is not enough to live a full life. There are some problems that people can have with their wheelchairs. The first is mobility. It implies moving or lifting a user. Then, it is its adaptability to different people with various diseases. After that, protection problems related to weather or night security. Currently, the connection to the network is very important. Next, it is maintenance. Technical support is a necessary part of using a wheelchair. Finally, all decisions should be within law.

This article describes the concept of full autonomy for people with limited mobility, which can also be used for the entire population.

Concept Modern technologies offer people with poor mobility an innovative wheelchair. There are many different wheelchairs. For our purpose, we need to consider the best version of a wheelchair with all possible options. Figure 1 presents a prototype of SCEWO wheelchair [1].



Fig. 1. SCEWO wheelchair

It has two big wheels to drive around on a flat ground, and the robustness of tracks to overcome curbs and climb stairs is unique. The rubber tracks allow the user to smoothly go up and downstairs in a safe manner. The change in the modes between the staircase and the surface is done automatically. This vehicle has a lot of necessary facilities but not all. It does not have any protection from adverse weather conditions and the navigation system. Besides, the maximum speed is not very high.

Another example is presented in Fig. 2. It was developed by Absolute Design and is called EQUAL, which is a compact single city car, designed for people moving in wheelchairs. This example also has advantages and disadvantages [2].

A man with disabilities wants to be independent. It makes it difficult to design a universal vehicle. If a person is at home, he should be able to take any object and easily go to bed and toilet. If he is outside, he must be able to go where he wants under any weather condition.

To create a hybrid vehicle for full autonomy we need to use the advanced technology. It must be small enough for good maneuverability inside buildings, but it must also have good functionality to perform many tasks. Thus, we offer to design a vehicle consisting of two parts. The first, and also the main part, is intended for moving inside the apartments, the

second one will expand the functionality of the first for moving in the street.



Fig. 2. EQUAL car

Conclusion. We want to create a universal hybrid car for people with limited mobility, like the Swiss army knife, which will offer increased mobility with all the necessary, up-to-date functions in one vehicle.

The convertible vehicle adapts to the user's parameters, which allows people with limited mobility to buy only one vehicle for the entire lifetime.

Thanks to the evolution of batteries, which have been reduced in their size and weight, the car will offer exceptional autonomy and ease. Protected and safe, the user can move around in the car thanks to protection from rain and cold.

In addition, the user will be at the forefront of digital development. The car will be autonomous and equipped with GPS; it will avoid accidents. Connection to the internet will allow it to communicate with different services increasing the comfort of the users.

REFERENCES

1. SCEWO. The Scewo wheelchair [Electronic resource]. – Access: <https://scewo.ch/> (reference date: 01.03.2018).
2. Blog about rehabilitation. City car for disabled people [Electronic resource]. – Access: <http://tvoishag.com/gorodskoj-avtomobil-dlya-invalidov.html> (reference date: 01.03.2018).

INFORMATION AND COMMUNICATION AREA

Bouchery Corentin, student

*Academic advisor E.M. Pokrovskaya, Associate Professor, PhD candidate
Tomsk, TUSUR, Corentin.bouchery@laposte.net*

First, it is important to understand what information and communication technologies (ICT) are. It's a term for computer, audio-visual, multimedia, internet and telecommunications platforms that allow users to communicate, access information sources, store and transmit information in any form: text, music, sound, image, video ...

Today, communication and information sharing are the main pillars of our society (economic, health, education, security, relational, dissemination of cultural property, land management, transport, environment, rights of persons with disabilities). Everything thanks through communication. In today's fast-paced world, the means of communication have had to evolve... We have moved quickly from the oral to writing and printing for mass distribution. Subsequently, the creation of electric lines allowed the appearance of the telegraph, the telephone and the radiotelephony. Computers has seen the day thanks to printed circuits. Television, Minitel, Internet and mobile telecommunications have made it possible to send images in addition to text and speech. In order to become even more efficient, combined devices (ex: the telephone) were equipped with cameras and internet access.

The miniaturization of components makes it possible to produce «multifunctional» devices at affordable prices as early as the 2000s. The rapid increase in the number of high-speed internet access (with ADSL or with satellite) and access to very high-speed internet (fibre optic) facilitated the broadcasting of audio-visual content at affordable prices, making each person then the owner of a telephone. Many social networks then appeared seduced millions / billion users creating multiple impacts on the functioning of society [1].

I Goal tree

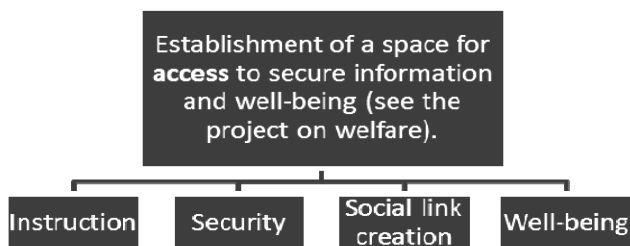


Fig. 1. Goal tree

II Project development. The purpose of this project is to create an innovative space for Information and Communication Technologies. To do this, rooms will be equipped with various equipment (computers, television, tablets, books). The main objective will be to allow learning using a maximum of different communication media (paper, digital, tactile, sound, tangible, visual, sensory). Through these arrangements, workshops and activities around the theme of communication can be realized such as correspondence with abroad, groups of words and proposals for activities, awareness of evolution and history communication media, creating comfortable space (Snoezelen space). A radio channel and a newspaper could also be created (radio club, newspaper, reporter ...) [2].

III Description piece by piece:

Multimedia Space: This piece will be dedicated to the use of computer and multimedia tools. It will discover new material and a new dimension of use. All systems will be equipped with Internet access and will be the focus of workshops on foreign correspondence. Users will also can bring their own work equipment.

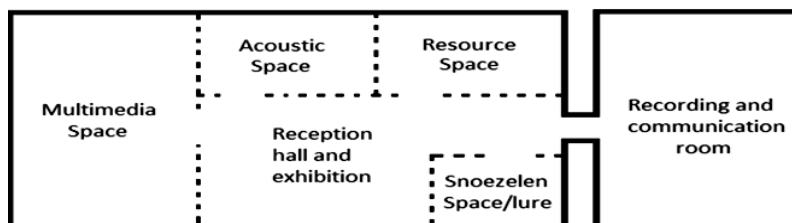


Fig. 2. Development area

Acoustic space: This room will be dedicated to students who need silence or music to work. Material for listening to music will be made available. A television will also be installed to take knowledge of the information. The communication media are here sound and visual (audiovisual).

Documentary resource space: This piece will allow to find documentary resources (magazines, newspaper, magazines, novel, dictionary, encyclopaedia ...) paper. The counselor will be able to inform the person according to these needs and the type of document required. Here, the communication medium will be paper. (Paper document, reading support).

Space of relaxation (Snoezelen space) / reading: This space will be made available to the students to make them live a sensory experience. Often students are stressed by their studies. This space will be an opportunity to study in better conditions. It is also a good place to read documents borrowed from the document resource space. Here, the communication medium is sensory.

Radio / reportage / meeting room: This room will have the theme «medias». Indeed, thanks to its technical equipment, it will allow student volunteers to set up a journalism club at the University of TUSUR. They will have equipment to create a radio channel and create a newspaper. Regular meetings may be held to distribute work tasks and communicate on the elements to be published. Here, the communication medium is radio, visual and press and oral. This is the room where the most communication support is implemented. This piece is composed of microphones projector, projection board, printer for newspapers [3].

Telecommunication discovery (exhibition): This adroit one will have several roles in the project. It will serve all parts. A counselor will be present to advise the students on their search for what they need. An exhibition to trace the evolution of Information and Communication Technologies will be exposed. Guided tours or events can be organized here.

IV Evolution and evaluation of the project. This project has the particularity of being scalable. It therefore can adapt to the remarks of students and users. For this reason, in a choice to adapt to student demand, an information questionnaire will be used for them. New technological advances will soon see the day and take place in this project.

REFERENCES

1. Gorana Celebic, Dario Ilija Rendulic. Basic Concepts of Information and Communication Technology. – Zagreb, 2011. – 86 p.
2. Armand Colin. Revue d'Économie Régionale & Urbain 2001/1 (février) // [Digital source]. – Digital journal. – 2001. – URL: <https://www.cairn.info/revue-d-economie-regionale-et-urbaine-2001-1-page-135.htm> (the date of access: 12.03.2018).
3. Craig Van Slyke. Information and communication technologies: concepts, methodologies, tools and application // Northern Arizona University. – 2008. – P. 523–525.

THE WELLBEING ENVIRONMENT

Florian Guerin, student

*Academic advisor E.M. Pokrovskaya, Associate Professor, PhD candidate
Tomsk, TUSUR, florian.guerin36@gmail.com*

To realize my article, I relied on a method of research and analysis of the situation in order to release the needs and to be able to set up solutions.

First, we must know that the notion of well-being is a notion that man has developed as he evolves to a central point in his life. Indeed, when men were nomadic, they sought mainly to meet the physiological needs having to feed, hydrate, all simply must survive (see Fig. 1. The pyramid of

Maslow). But little by little, men have evolved and with the development of agriculture they have found a reliable way of being able to keep food nearby and thus avoid the displacement that imposing the gathering or the hunting. As a result, men began to create communities (villages) and interactions between them as they realized that many were stronger and less susceptible to hazards. Their standard of living and thus their requirement are thus mounted in the matter of need passing to the second, stage that of the security. Once these steps have been completed, we reach the stages that consider the notion of well-being such as social needs, self-esteem and personal fulfillment.

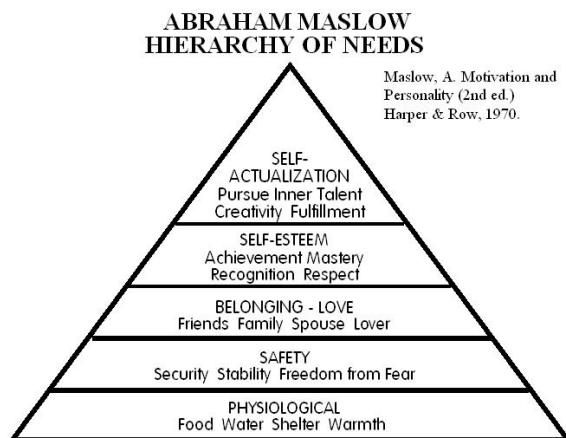


Fig. 1. Pyramid of Maslow

But finally, how can one precisely define what is well-being?

Well-being is a state linked to different factors considered separately or jointly with health, social or economic success, pleasure, self-realization, harmony with oneself and with others.

The term welfare refers to two main designations:

- a first is physical: the physical well-being is defined by the feeling of a general good physiological health, a satisfaction of the primordial needs of the body;
- a second refers to the psychological well-being that comes from a personal and subjective evaluation. Which can come from different perceptions or satisfactions, financial, professional, sentimental but also from the absence of mental disorders. The general notion of malaise is often presented as defining the opposite situation.

We can therefore have several approaches to well-being, a lifestyle approach, one on health, one on work, one on the economy and one on so-

ciety. But I decided to develop an aspect of well-being that by my position and my age affects me more particularly, it is the well-being at the university or at school in general. In addition, it is important to enable youth education to develop a future society that is more inclined to be in good shape physically and morally.

To begin, we will first make a quick statement of the perception of wellbeing in different countries. There are currently few countries where there are tools to consider the wellbeing, but in France a study realized by CREDOC has been done (see reference n°1). Although the French are often described as a sullen and grouchy people, perpetually dissatisfied with their situation. Yet when asked, 33% say they are "very often" happy, 47% "often happy» (Fig. 2. Representation of the state of mind of the French). In all, eight out of ten French people feel satisfied with their lives [1].

Representation of the state of mind of the French

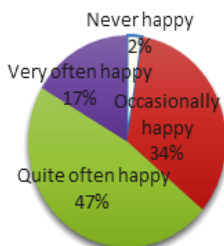


Fig. 2. Representation of the state of mind of the French

The range of reasons for happiness mentioned by the French is very wide and no less than thirty reasons are mentioned in the various surveys that can be found, ranging from «sun» to «nature», through «retirement» or «freedom», etc. But three main reasons are mentioned revolving around emotional ties: children, family or the couple. Depending on the age it was not the same relations that are evoked, the youngest find happiness in an expanded relationship circle (which also integrates friends), and over time, happiness finds its source more and more within the nuclear family (close family). Another source of well-being that comes up often is work that is a source of happiness and hobbies are then mentioned. Although the financial situation or health is not often mentioned as a reason to be happy today, it seems to be seen more as a means of improving well-being. Conversely, financial insecurity and poor health are the two main drivers of misfortune. In other words, money problems or health problems are a serious obstacle to happiness but having income or good health cannot alone be the source of happiness.

Problem. Indeed, if it is so important to be able to consider the well-being of young people and adolescents it is that it has a major impact on their personal development. The consequences of an ill-being can indeed be multiple. From stress to insomnia, the demonstrations can go as far as the suicide attempt.

Stress, a growing concern. Currently, the main source of harm in our environment is the creation of stress, it is the latter that is the center of my thinking and it is necessary to define well and understand this.

We must start by saying that there are two different types of stress and that it is not always a bad thing. Stress is a natural phenomenon that can alert our body to the various hazards that may occur, in small doses it can therefore improve these performances. For example, a low amount of stress will encourage a student to study more and to pass these exams better. This is called positive stress. It adds a short-term tension to the body that gives it an extra boost of adrenaline to overcome a challenge.

The fact is that when we are stressed we often don't take the time to evaluate our choices as we would normally, under stress have a tendency to rush and to carry out actions that are not necessarily the right ones and that can even be dangerous for the stressed individual in himself or for the people around him. For example, it is possible that we take a taxi when we can ride a bike or choose the first thing on the shelf of the supermarket even if it is not what we wish or have trouble in talk and not succeed in expressing these real thoughts when you must speak in public [2].

In France, according to a recent study by the Organization for Economic Co-operation and Development, schoolchildren are more affected by stress than in any other industrial country. About students, the results of a national survey conducted by regional student associations in 2006 found that 43.6% of students reported suffering from one of the three symptoms of depression: a feeling of sadness, a lack of self-confidence or suicidal thoughts. Adolescents who try to cope with mental distress are often more likely to be addicted (tobacco, cannabis or alcohol). This picture is not much brighter for people at work. According to the French Institute for Action against Stress (IFAS), excessive stress at work affects more than 32% of women and 20% of men.

Between parents, worried about the future of their offspring from the beginning of kindergarten, overloaded programs and not always adapted to the needs of children, the school has become a stressful place. Still, it could also be the perfect place to start easing stress and better prepare future generations to cope with this scourge of modern life.

But why is stress dangerous for current generations?

Stress reduces the quality of sleep. Stress makes students more anxious. Stress also has a negative impact on educational results.

And finally, in the most severe cases, stress can lead students to commit suicide. There are some countries where the number of suicide is particularly important among students; this is particularly the case in Japan or India. The number of suicides in Indian higher education institutions continues to increase. He is close to 10,000 in 2016 alone and school failure is the first cause. It is defined that a student commits suicide per hour now. This high rate of suicide is alarming, and the majority due to stress and academic failure, but also the fact that one pushes more and more young people to academic excellence, is to be taken into consideration. This is also often due to breakup and loss and social isolation [3].

Towards an improvement of well-being with new technologies?

In today's world, with the evolution of new technologies is developing new solutions to reduce stress and the creation of helmets to create a virtual environment. Indeed, the helmets currently on the market such as the Oculus Rift, the PlayStation VR or the HTC Vive can plunge the user into a game and we can imagine that this game has relaxing features and allow you to relax [4].

I concluded that a relaxation room could really have positive effects on the well-being of students and I thus analyzed what is already set up such as in Kentucky where it has already been put in place. In order to better adapt it, I chose to create a questionnaire for students and teachers so that this room is adapted to the desires and needs of TUSUR University. Relaxation comes from deliberate attention to our mind and body through a variety of skills and practiced activities.

The relaxation room must therefore be a place where it is possible to practice a variety of activities that can soften or soothe stress or other difficulties that may be encountered. Some of his skills are geared towards calming the mind and slowing down our thinking. Others incorporate physical relaxation or body stimulation [5].

REFERENCE

1. Régis Bigot, Patricia Crouette, Emilie Daudey, Sandra Hoibian, Jörg Mülle, CREDOC, research notebook. The evolution of wellbeing in France for 30 years. – URL: www.credoc.fr, N°298, (the date of access: 05.03.2018).
2. Philippe Testard-Vaillant, CNRS international magazine.Stress, the Bane of Modern Life. – URL: <http://www2.cnrs.fr/en/1070.htm>, date : (the date of access 05.03.2018).
3. INRS (National Research and Safety Institute) health and security at work, Folder «Stress at work», URL :<http://www.inrs.fr/risques/stress/effets-sante.html>, the date of access: 05.03.2018).
4. Le Monde, «A nap room for exhausted students», URL: http://www.lemonde.fr/campus/article/2017/02/07/une-salle-pour-rejoindre-les-bras-de-morphee-a-l-universite_5076002_4401467.html, (the date of access: 05.03.2018).
5. University of Kentucky, «Relaxation Room». – URL :<http://www.uky.edu/counselingcenter/relaxation-room-1>, (the date of access: 05.03.2018).

КРУГЛЫЙ СТОЛ

«ИНТЕГРАЦИЯ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ И РЕСУРСОВ ШКОЛЫ, ТЕХНИКУМА И ВУЗА В ЦЕЛЯХ ПОВЫШЕНИЯ КАЧЕСТВА НЕПРЕРЫВНОЙ ПОДГОТОВКИ СПЕЦИАЛИСТОВ»

КРУГЛЫЙ СТОЛ

«ИНТЕГРАЦИЯ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ И РЕСУРСОВ ШКОЛЫ, ТЕХНИКУМА И ВУЗА В ЦЕЛЯХ ПОВЫШЕНИЯ КАЧЕСТВА НЕПРЕРЫВНОЙ ПОДГОТОВКИ СПЕЦИАЛИСТОВ»

МОДЕЛЬ ШКОЛЬНОГО ТЕХНОЛОГИЧЕСКОГО ОБРАЗОВАНИЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ НАПРАВЛЕННОСТИ НА ОСНОВЕ СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ «ШКОЛА – ВУЗ – ПРЕДПРИЯТИЕ»

В.В. Горовцова, зам. директора по МиИР

г. Томск, ОГБОУ «Томский физико-технический лицей»

Приоритетной задачей подготовки кадров для высокотехнологичных предприятий является мотивированный выбор выпускниками школ инженерно-технического образования и получения ими высоко-го профиля инженерных компетенций. Уровень развития инженерных компетенций зависит от содержания, необходимости и достаточности полученных знаний, навыков, умений.

В ОГБОУ «Томский физико-технический лицей» разработана и апробируется модель школьного технологического образования, направленная на развитие технических способностей, знакомство с инженерными профессиями и ориентацией школьников на инженерно-техническое образование.

Цели технологического образования в лицее:

1. Овладение учащимися методами проектирования, моделирования, конструирования, учебно-исследовательской и проектной деятельности.
2. Приобретение учащимися навыков работы с учебным оборудованием.
3. Приобретение опыта практического решения инженерно-технических задач.
4. Стимулирование интереса учащихся к сфере инноваций и современных технологий.
5. Знакомство с требованиями социально-культурного пространства высокотехнологичных промышленных предприятий в регионе.

6. Ранняя профориентация и личностное самоопределение учащихся.

В лицее по инициативе попечительского совета с марта 2016 г. реализуется проект по созданию системы непрерывного базового и целевого инженерно-технического образования на основе трехзвенного взаимодействия «школа – вуз – предприятие». Участниками проекта стали: ОГБОУ «Томский физико-технический лицей» – ТУСУР – Научно-производственная фирма «Микран».

В рамках трехстороннего проекта «Созвездие» на базе Лицея создана кафедра ТУСУРа по инженерной подготовке учащихся. На кафедру зачисляются на добровольной основе и по согласованию с родителями учащиеся 6–11 классов, мотивированные к дальнейшей технической деятельности, конструированию, исследованию и изобретательству.

Основные направления работы кафедры:

- реализация инновационных программ дополнительного образования по трем направлениям: робототехника, программирование и микроэлектроника.

- лекторий: знакомство с приоритетными направлениями развития науки, технологий и техники;

- мастер-классы технической направленности, которые проводятся в течение всего учебного года;

- вовлечение одаренных учащихся в инновационную деятельность на базе вузов по направлениям, связанным с основами технологических процессов, с использованием технологии группового проектного обучения. Темы проектов не оторваны от жизни, они реальны и безопасны. В группы могут входить как учащиеся, так и студенты 2, 3-го курсов. Групповой проект выполняется в лабораториях ТУСУРа, ЦМИТа, НПФ «Микран».

- встречи с приглашенными представителями предприятий вне региона;

- проведение летних профессионально-ориентированных практик в лабораториях и центрах вуза, на предприятии, направленных на формирование первичных профессиональных знаний и умений. Предусматривается публичная защита результатов практик.

- проведение летних практик совершенствования английского языка преподавателями вуза (разговорный и технический английский язык);

- участие учащихся в образовательных и социальных мероприятиях вуза.

Реализация проекта сетевого взаимодействия школа – вуз – предприятие предполагает серьезное расширение образовательной среды

для учащихся, увеличение возможностей для осуществления проб и личностного самоопределения в области инженерно-технического знания. В таких условиях становится очевидной необходимость осуществления особого вида психолого-педагогического сопровождения, обеспечивающего навигацию в образовательной среде, построение и реализацию индивидуального маршрута образовательного движения ученика на весь период его обучения на кафедре инженерной подготовки. Психолого-педагогическое сопровождение является важным условием для формирования мотивации и ценностно-смысловых ориентиров, влияющих на дальнейший выбор профессионального образования. «Портфолио», как технология личностного развития, выбрана одним из ведущих инструментов психолого-педагогического сопровождения, которое осуществляют психолог и классные руководители.

Совокупность перечисленных видов деятельности обеспечивает формирование у учащихся:

- навыков технического мышления (понимание механико-технических соотношений, гибкость мышления, особенности отражения физических явлений и законов, конструкторская фантазия);
- ресурсов практических умений, опыта;
- инициативности;
- мотивированного профессионального самоопределения.

**МОДЕЛЬ ШКОЛЬНОГО ТЕХНОЛОГИЧЕСКОГО
ОБРАЗОВАНИЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ
НАПРАВЛЕННОСТИ НА ОСНОВЕ СЕТЕВОГО
ВЗАИМОДЕЙСТВИЯ «ШКОЛА – ВУЗ – ПРЕДПРИЯТИЕ»**

Е.Е. Макарова, зам. директора по развитию;

*Ю.В. Храмовских, учитель русского языка и литературы
г. Томска, МАОУ СОШ №19*

ФГОС нацеливают нас на формирование и развитие личностных, метапредметных и предметных результатов. При этом «...запрос на индивидуализацию и тьюторское сопровождение не всегда формулируется напрямую, тем не менее, распространена формулировка через образовательные результаты, которые возможны лишь при индивидуализации образовательного процесса и тьюторском сопровождении»[1]. На сегодняшний день в сознании большинства педагогов школы есть понимание новой роли учителя – навигатора, проводника в океане информации, сопровождающего ученика на его пути, который он выбирает сам. Система индивидуализации образования включает

три основных элемента, в которой ученик развивается с первого по выпускной класс [2]. Первый элемент – авторский сквозной курс практической философии «Я – система в системе мира». Курс вводит в открытое образовательное пространство единый конфигуратор – понятийный аппарат, позволяющий понимать друг друга всем субъектам. Дорожные карты самоопределения учащихся – технология формирования, самопроектирования и развития личностных результатов учащимися и одновременно система мониторинга личностных результатов. Форум проектов – пространство культивации и развития жизнеспособных идей школьников. Это ежегодный фестиваль с международным участием, в котором жюри – представители тех сфер деятельности, в которых предполагают внести изменения участники с помощью продуктов своих проектов. Анализ образовательных результатов контрольных групп проекта доказывает результативность и эффективность системы. Так, выпускники 2017 г. (11 класс) как и выпускники 9 класса в 2016 г. – 100% поступили куда планировали (вузы Томска и Омска, колледжи и техникумы Томска) и довольны процессом своего образования. Девятиклассники – выпускники 2016 г. участвовали в Открытом Форуме проектов с международным участием в прошлом году уже как студенты-волонтеры, а в 2018 г. по своей инициативе планируют открыть на Форуме новое направление – защита проектов студентов СПО. В системе предпрофильной подготовки успешно развиваются по индивидуальным образовательным траекториям группы будущих медиков (в сотрудничестве с СибГМУ), ребята проводят исследования под кураторством преподавателей вуза и занимаются на лекциях на разных кафедрах. Бланков дорожных карт оказалось недостаточно, и они инициировали тетради самообразования как приложения к картам. Взаимодействие установлено со всеми вузами города: на всех уровнях школьного образования. Взаимодействие с НИ ТПУ (более ста учащихся занимаются в сетевых проектах), с НИ ТГУ активно взаимодействуют группы НОО (также более ста учащихся). В активном режиме ведутся разработки образовательных траекторий с ТУСУР и ТГАСУ, которыми также заинтересованы учащиеся на всех уровнях школьного образования. Систематически проходят профессиональные пробы в центре планирования карьеры. Образовательная инициатива, представленная МАОУСОШ №19 г. Томска на защите региональных тьюторских практик в июне 2017 г., прошла экспертизу межрегиональной тьюторской ассоциации. Данная инициатива была сертифицирована как соответствующая корпоративному стандарту МТА и рекомендована для тиражирования на федеральном уровне, а также рекомендовано муниципальным и ре-

гиональным органам управления образованием оказывать содействие в развитии и оформлении инициативы, обеспечить широкую презентацию инновационного опыта автора на территории. С 30 октября по 1 ноября 2017 г. ОГБУ региональный центр развития образования Томской области совместно с Центром этнокультурного образования школы организовал курсы повышения квалификации в формате стажировки по направлению формирования личностных результатов в соответствии с ФГОС. Результат стажировки – тиражирование технологии «Дорожная карта самоопределения учащегося». Систему сегодня успешно используют не только общеобразовательные школы (в частности, Могочинская школа Молчановского района Томской области), но и в пенитенциарной системе (МКОУ ВСОШ №8) и в системе дополнительного образования – ДК «Смена». В ноябре 2017 г. программа стажировки победила в муниципальном конкурсе стажировочных площадок.

ЛИТЕРАТУРА

1. Ковалева Т.М. Условия введения тьюторства в современной школе и основные схемы тьюторского сопровождения / Тематическая консультация по теме «Тьюторское сопровождение в условиях идеологии открытого образования» [Электронный ресурс]. – <http://edu.shd.ru/index.ptp?option>
2. Макарова Е.Е., Осипова Е.В., Ведерникова М.И. Методическое описание авторской технологии Е.Е. Макаровой «Дорожная карта самоопределения» // «Организация исследовательской деятельности детей и молодёжи: проблемы, поиск, решения». – Томск: Изд-во НИТПУ, 2017. – 299 с. [Электронный ресурс]. – <http://abiturient/tpu/ru/file/2018/docs/olimp/sbornic-tpu-na-sajt-2017-11-28.pdf>

СТАНОВЛЕНИЕ СИСТЕМЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОГО ОБРАЗОВАНИЯ В АКАДЕМИЧЕСКОМ ЛИЦЕЕ г. ТОМСКА им. Г.А. ПСАХЬЕ

***С.А. Калашиникова, учитель информатики и ИКТ
высш. квалификационной кат., зав. каф. физико-математических
и информационных дисциплин
г. Томск, МБОУ Академический лицей им. Г.А. Псахье***

Проблема качественного инженерно-технического образования стоит остро не только в России, но и во всем мире. Всё сильнее ощущается нехватка квалифицированных инженеров, способных не только внедрять в производство наукоёмкие технологии, но и разрабатывать их. Падение популярности объясняют тем, что инженерная деятельность ассоциируется с тяжелой и скучной работой, которая плохо оплачивается.

Школьники имеют очень слабое представление о современном производстве, даже поступая в вузы на технические специальности, они с трудом представляют себе свою будущую деятельность, что сказывается и на выборе направлений деятельности, и на мотивации к обучению, и зачастую, приводит к разочарованию, и, как следствие, уходу из профессии.

Во время одного из круглых столов в Томском университете систем управления и радиоэлектроники, где встречались работодатели, преподаватели вузов и школьные педагоги, были обозначены следующие проблемы, которые преследуют и выпускников вузов, и выпускников школ: отсутствие организаторских способностей, неумение работать в команде, неумение ясно излагать мысли, неумение лаконично писать, неумение работать с терминами, неумение решать нестандартные задачи, неумение ставить задачу, низкий уровень практических, измерительных, проектно-конструкторских навыков, и в целом, недостаточный уровень базовых знаний в естественно научном направлении.

Что же с этим делать? Необходимо менять подход к профессиональной ориентации школьников. А также уделять внимание комплексному развитию личности.

В Академическом лицее г. Томска традиционно сильным является физико-математическое образование. Шесть лет назад к нему добавилось новое направление информационно-технологическое, а в текущем учебном году был открыт инженерно-технический профиль. Эти три профиля и стали базой для подготовки выпускников лицея, нацеленных на получение образования современного, инновационного инженера. В основе лежат профильные предметы: физика, математика, информатика и ИКТ, робототехника и английский язык. Свободное владение английским языком в условиях все возрастающей глобализации становится неотъемлемой частью инженерного образования.

В рамках базовой учебной программы введён новый курс «Основы робототехники» для обучающихся 5–9-х классов. Педагогами составлены учебные программы, которые в настоящее время апробируются и дорабатываются.

Кроме этого, разработаны и внедрены программы элективных курсов: «Основы 3D-моделирования», «Персональный компьютер: настройка и поддержка», «Информационная безопасность. Основы криптологии», «Физика своими руками».

Базовый учебный план дополняют индивидуальные образовательные программы лицейстов (ИОП). Это обеспечивает дифференциацию учебных и профессиональных интересов обучающихся. ИОП

строится из набора специальных курсов, которые выбирает лицеист, например: «Углубленное изучение программирования», «Индивидуальная образовательная программа по физике», «Математический кружок: решение нестандартных задач», «Решение задач повышенной сложности по информатике», «Компьютерная графика и анимация», «Моделирование и программирование информационно-технических систем». На последнем остановимся подробнее. Этот курс включает в себя несколько этапов в зависимости от возраста ученика и рассчитан на обучающихся со 2-го по 11-й класс. Начинается курс обучения с основ конструирования и программирования простейших робототехнических систем и заканчивается применением микроэлектроники для разработки собственных конструкций с использованием различных микропроцессоров, созданием деталей с помощью 3D-принтера и написанием сложных алгоритмов, например, с применением теории искусственных нейронных сетей.

Индивидуальная образовательная траектория дополняется набором социальных практик и стажировок. У Академического лицея сложились партнерские отношения с рядом резидентов Томской технико-внедренческой зоны, которые заинтересованы в притоке молодых, перспективных кадров и поэтому с готовностью принимают старшеклассников на экскурсии, рассказывают о современных технологиях, демонстрируют оборудование, свои разработки, а также помогают советами и консультациями в некоторых проектах, разрабатываемых учениками лицея. Это инновационные предприятия, работающие в разных инженерных направлениях от области машиностроения, до технологий 3D-телевидения.

Многолетнее сотрудничество с Советом молодых ученых Томского научного центра складывается не только из экскурсий в различные лаборатории исследовательских институтов и лекций, но и участия молодых научных сотрудников в качестве экспертов в ежегодных научно-исследовательских конференциях обучающихся Академического лицея.

Кроме этого, мы, конечно же, используем потенциал высшей школы: мастер-классы, творческие встречи с преподавателями и выпускниками ТУСУРа, ИПМКН и механико-математического факультетов ТГУ, Института кибернетики ТПУ и др. помогают старшеклассникам понять особенности различных специальностей и особенности обучения. В течение 2-х лет Академический лицей участвует в сетевой программе ТГУ «Открытая STEM-лаборатория». STEM-образование – это один из основных трендов в мировом образовании (Science – естественные науки, Technology – технология, Engineering – инженерное искусство, Mathematics – математика).

Обязательной частью учебной программы в профильных классах является проектная деятельность. Проекты, разрабатываемые лицеистами, могут носить исследовательский или практический характер, результатом является защита проекта на научно-практической конференции.

Среди огромного количества всевозможных олимпиад и конкурсов, предлагаемых школьникам, мы проводим тщательный отбор и сосредотачиваемся только на тех, которые, на наш взгляд, «работают» на нашу цель – подготовку выпускников к осознанному выбору инженерных специальностей. В число таких олимпиад и конкурсов вошли те, которые развивают организаторские способности лицеистов, навыки групповой, командной работы, умение принимать ответственное решение в условиях ограниченного времени и ресурсов, умение кратко и точно формулировать ответ, находить оптимальное или нестандартное решение, а также способствуют общеинтеллектуальному развитию учеников, расширению их кругозора.

Необходимо отметить, что развитие инженерно-технического направления требует хорошей современной материальной базы. И как следствие, готовности образовательного учреждения к постоянной модернизации оборудования. Самостоятельно школе такую нагрузку не вынести, поэтому выстраивание партнерских отношений с бизнес-сообществом, родительской общественностью и депутатским корпусом является важным направлением работы администрации и коллектива лицея.

К настоящему моменту в Академическом лицее оборудована современная физическая лаборатория и лаборатория робототехники. Это позволяет организовать работу обучающихся на уроках физики и информационных технологий на новом качественном уровне, а также обеспечивает массовый охват тех, кто хотел бы попробовать себя в области робототехники, конструирования и моделирования.

Одной из серьезных проблемных зон в инженерно-техническом направлении в школе является острая нехватка готовых учебных и методических разработок. Поэтому педагогам необходимо постоянно искать возможности для повышения квалификации и обмена опытом.

Система инженерно-технического образования в Академическом лицее еще не сложилась окончательно и находится в стадии активного становления, хотя уже есть результаты – более 50% выпускников лицея выбирают инженерно-технические специальности.

Таким образом, подводя итог вышесказанному, отмечаем, что только комплекс мер может привести к желаемому результату.

СОДЕРЖАНИЕ

СЕКЦИЯ 4

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ПОДСЕКЦИЯ 4.1

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

*Председатель секции – Шелупанов А.А., ректор ТУСУРа,
директор ИСИБ, д.т.н., проф.;*
зам. председателя – Конев А.А., доцент каф. КИБЭВС, к.т.н.

Т.С. Косаченко, М.А. Андреев

НАПИСАНИЕ ПРАВИЛ НОРМАЛИЗАЦИИ И КОРРЕЛЯЦИИ ДЛЯ
ВЫЯВЛЕНИЯ СЛЕДОВ АРТ ПРИ ПОМОЩИ MAХRATROL SIEM..... 13

Д.А. Антипов

СОВРЕМЕННЫЕ ПОДХОДЫ К СНИЖЕНИЮ ПОКАЗАТЕЛЯ
СИГНАЛ-ШУМ В КАНАЛЕ УТЕЧКИ ПЭМИ..... 15

А.Е. Гуськов, А.И. Дзангиев, М.А. Першин

ПРОГРАММНО-АППАРАТНЫЕ КОМПЛЕКСЫ «БЛОКХОСТ» 18

А.А. Бедарева, А.А. Колесникова, М.А. Куртова

ПРИМЕНЕНИЕ ЗНАКОВЫХ ГРАФОВ И ТЕОРИИ
СТРУКТУРНОГО БАЛАНСА ДЛЯ ПОСТРОЕНИЯ
МОДЕЛИ ИНФОРМАЦИОННОЙ ВОЙНЫ 20

Ф.И. Кропочев, Д.А. Мех, А.А. Исанов

ОСНОВНЫЕ УГРОЗЫ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ
И МЕТОДЫ ЗАЩИТЫ ОТ НИХ 23

А.С. Кокурина, В.С. Мельман

ОБЗОР ПОДХОДОВ К ВЫБОРУ НАИЛУЧШЕГО
ИЗОБРАЖЕНИЯ-КОНТЕЙНЕРА ДЛЯ СТЕГАНОГРАФИЧЕСКОГО
ВСТРАИВАНИЯ ИНФОРМАЦИИ 26

П.В. Перминов, П.А. Ковчунов

РАЗРАБОТКА КУРСА ПРАКТИЧЕСКИХ ЗАНЯТИЙ
ПО ДИСЦИПЛИНЕ «БЕЗОПАСНОСТЬ СЕТЕЙ ЭВМ» 29

А.Я. Бомбов, А.С. Репкин, А.В. Кравцова

РАЗГРАНИЧЕНИЕ ДОСТУПА К ИНФОРМАЦИИ
В СИСТЕМЕ MOODLE 32

А.А. Михайлова

ЗАЩИТА ИНФОРМАЦИИ В ОПЕРАЦИОННЫХ СИСТЕМАХ
СЕМЕЙСТВА LINUX 35

Н.В. Петров

МЕТОДИКА ОПИСАНИЯ ЗАЩИЩАЕМЫХ РЕСУРСОВ,
ИСПОЛЪЗУЕМЫХ ПЕРСОНАЛОМ..... 37

Р.П. Попадинец СИСТЕМА АУТЕНТИФИКАЦИИ ОБЪЕКТОВ ПРОМЫШЛЕННОЙ СЕТИ	40
К.О. Семьехина ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ ВЕБ-ПРИЛОЖЕНИЙ И МЕТОДЫ ЗАЩИТЫ ОТ НИХ	42
О.О. Шумская СРАВНИТЕЛЬНОЕ ИССЛЕДОВАНИЕ МЕТОДОВ КЛАССИФИКАЦИИ В СТЕГОАНАЛИЗЕ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ПРИЗНАКОВ В ЧАСТОТНОЙ ОБЛАСТИ	45
Д.С. Световец, Е.Ю. Костюченко НАПОЛНЕНИЕ И ПРЕДОБРАБОТКА БАЗЫ ДАННЫХ КЛАВИАТУРНОГО ПОЧЕРКА	49

ПОДСЕКЦИЯ 4.2

РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ И СРЕДСТВА ИХ ЗАЩИТЫ

*Председатель секции – Голиков А.М., доцент каф. РТС, к.т.н.; зам.
председателя – Бернгардт А.С., доцент каф. РТС, к.т.н.*

Н.Е. Аносинская, О.С. Каймонов ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ СИСТЕМЫ АНТИКРИЗИСНОГО УПРАВЛЕНИЯ МЧС РОССИИ.....	53
Р.В. Блесков РАСПОЗНАВАНИЕ ЛИЦ ЛЮДЕЙ ПО СИГНАЛАМ С КАМЕРЫ ВИДЕОНАБЛЮДЕНИЯ.....	56
С.Р. Еремеев РАЗРАБОТКА ЛАБОРАТОРНО-ПРОГРАММНОГО КОМПЛЕКСА И УЧЕБНО-МЕТОДИЧЕСКОГО ПОСОБИЯ ДЛЯ ИЗУЧЕНИЯ ПРИНЦИПОВ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ	59
А.О. Эрлих, А.В. Тетерлева ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ИЗУЧЕНИЯ ПЕРСПЕКТИВНЫХ МЕТОДОВ КОДИРОВАНИЯ.....	62
О.Ю. Григорьев ДИДАКТИЧЕСКИЙ МОДУЛЬ «КОДЕК РИДА–СОЛОМОНА (7,3)»	65
А.С. Храмов МОДЕЛЬ АДАПТИВНОЙ ДВУСТОРОННЕЙ ШИРОКОПОЛОСНОЙ СПУТНИКОВОЙ СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ	67
П.А. Иванов РАЗРАБОТКА СИСТЕМЫ РАДИОСВЯЗИ ПОВЫШЕННОЙ ДАЛЬНОСТИ ДЕЙСТВИЯ ДЛЯ БПЛА SUPERCAM–350	71

К.Д. Карпачев СИСТЕМА МОБИЛЬНОЙ СВЯЗИ ДЛЯ АНПА «ГЛАЙДЕР» НА БАЗЕ ГРУППИРОВКИ НИЗКООРБИТАЛЬНЫХ СПУТНИКОВ «ГОНЕЦ-ДИМ»	74
Д.В. Дудкин, М.Д. Медведев СИСТЕМА НЕЙРОСЕТЕВОЙ ОБРАБОТКИ ИЗОБРАЖЕНИЙ РЕЧНОГО РАДИОЛОКАТОРА	77
А.В. Кригер МОДЕЛЬ СИСТЕМЫ МОБИЛЬНОЙ СВЯЗИ СТАНДАРТА IEEE 802.16 (WiMAX) НА БАЗЕ ПО МАТЛАВ	80
А.С. Кудряшов СИСТЕМА ПЕРЕДАЧИ ДАННЫХ САМООРГАНИЗУЮЩЕЙСЯ СЕТИ БАЛЛИСТИЧЕСКИ СВЯЗАННОЙ ГРУППЫ МАЛЫХ КОСМИЧЕСКИХ АППАРАТОВ НА БАЗЕ СТАНДАРТА IEEE 802.16M	83
В.А. Лобов МОДЕЛИРОВАНИЕ И ИССЛЕДОВАНИЕ ГЕНЕРАТОРА ПСЕВДОСЛУЧАЙНЫХ СИГНАЛОВ НА ОСНОВЕ НЕЛИНЕЙНЫХ ДИНАМИЧЕСКИХ СИСТЕМ ЛОРЕНЦА	86
М.Д. Медведев и В.С. Кралинов МОДЕЛЬ МОДУЛЯТОРА APSK В LABVIEW	88
А.С. Никонов ВЕЙВЛЕТ-ФИЛЬТРАЦИЯ СИГНАЛОВ МОРСКОГО РАДИОЛОКАТОРА НА ФОНЕ ВЗВОЛНОВАННОЙ МОРСКОЙ ПОВЕРХНОСТИ.....	91
Д.М. Орлов СИСТЕМА ПЕРЕДАЧИ ДАННЫХ ДЛЯ «РОЯ» НАНОСПУТНИКОВ CUBESAT 3U НА БАЗЕ СТАНДАРТА IEEE 802.16M	94
М.С. Смолин, Ю.С. Хило ЗАЩИЩЕННАЯ MESH-СЕТЬ ДЛЯ «РОЯ» БПЛА	97
А.Р. Усманова АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС QNAP NS-256-PRO+ И WEB-САЙТ «СИСТЕМОТЕХНИКА РТС».....	99
Д.А. Ишмуков МОДЕЛИРОВАНИЕ И ИССЛЕДОВАНИЕ ГЕНЕРАТОРА ПСЕВДОСЛУЧАЙНЫХ СИГНАЛОВ НА ОСНОВЕ НЕЛИНЕЙНЫХ ДИНАМИЧЕСКИХ СИСТЕМ ЧУА	102

ПОДСЕКЦИЯ 4.3

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

*Председатель секции – Кузьмина Е.А., доцент каф. КИБЭВС, к.т.н.; зам.
председателя – Глухарева С.В., ст. преп. каф. КИБЭВС*

М.Е. Абросимова БЛАГОНАДЕЖНЫЙ СОТРУДНИК В СИСТЕМЕ КАДРОВОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ	105
--	-----

А.А. Червинская МЕТОДЫ МИНИМИЗАЦИИ РИСКОВ КРЕДИТОВАНИЯ ФИЗИЧЕСКИХ ЛИЦ.....	108
А.В. Куртукова, П.А. Дятлова, А.С. Романов АНАЛИЗ СОВРЕМЕННЫХ СРЕДСТВ ПОЛУЧЕНИЯ КРИПТОВАЛЮТ ...	111
А.Г. Вахитов, М.М. Джаналиев, Ю.А. Рубцова, А.С. Колтайс ВНЕДРЕНИЕ ИНФОРМАЦИОННО – АНАЛИТИЧЕСКОЙ СИСТЕМЫ «СПАРК» В УЧЕБНЫЙ ПРОЦЕСС ФАКУЛЬТЕТА БЕЗОПАСНОСТИ	114
В.Е. Мальцев, А.С. Еременко, А.О. Селезнев, С.В. Глухарева РЕКОМЕНДАТЕЛЬНАЯ СИСТЕМА КАДРОВОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ.....	116
И.В. Крист, С.В. Глухарева МЕТОДИКА ОЦЕНКИ НА ЭТАПЕ ПОДБОРА ПЕРСОНАЛА В СИСТЕМЕ КАДРОВОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ.....	118
В.А. Кудрявцева ТЕНЕВАЯ ЭКОНОМИКА КАК УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ СТРАНЫ	121
М.О. Мамскова БЛОКЧЕЙН КАК ПОМОЩНИК В ОБЕСПЕЧЕНИИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ	124
Н.Н. Манчилаева УГРОЗА ОТКЛЮЧЕНИЯ РОССИЙСКИХ ОРГАНИЗАЦИЙ ОТ СИСТЕМЫ SWIFT. ПЕРСПЕКТИВЫ РАЗВИТИЯ СИТУАЦИИ	128
Е.В. Мареева МЕТОД АНКЕТИРОВАНИЯ НА ЭТАПЕ ПОДБОРА ПЕРСОНАЛА В СИСТЕМЕ КАДРОВОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ.....	131
О.И. Маркова ОЦЕНКА ЭФФЕКТИВНОСТИ ВЫПОЛНЕНИЯ АДРЕСНЫХ ПРОГРАММ ЖКХ ПО ПРОВЕДЕНИЮ КАПИТАЛЬНОГО РЕМОНТА В МНОГОКВАРТИРНЫХ ДОМАХ	133
П.Н. Орлихина ВЛИЯНИЕ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ ТОМСКОЙ ОБЛАСТИ.....	136
Н.В. Петрова БЛОКЧЕЙН В ЦИФРОВОЙ ЭКОНОМИКЕ: ПРЕИМУЩЕСТВА И ПРОБЛЕМЫ	138
П.В. Прокушев, М.М. Джаналиев, А.С. Колтайс, Ю.А. Рубцова АНАЛИЗ СПЕЦИАЛИЗИРОВАННЫХ ИАС ДЛЯ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ.....	141
И.А. Готфрид, Е.С. Линенко, Е.Ю. Складанюк БАНКРОТСТВО КАК ИНСТРУМЕНТ УХОДА ОТ УПЛАТЫ НАЛОГОВ.....	145

А.А. Воронович НОВЫЙ ПОДХОД К ОЦЕНКЕ ПЕРСОНАЛА В СИСТЕМЕ КАДРОВОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ.....	147
--	-----

В.Ю. Арвачёв, Д.Б. Жалсанова РЕЗУЛЬТАТИВНОСТЬ НАЛОГОВЫХ ПРОВЕРОК И СОВЕРШЕНСТВОВАНИЕ МЕХАНИЗМА ИХ ПРОВЕДЕНИЯ	149
---	-----

СЕКЦИЯ 6

ЭКОЛОГИЯ И МОНИТОРИНГ ОКРУЖАЮЩЕЙ СРЕДЫ. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

Председатель секции – Карташев А.Г., проф. каф. РЭТЭМ, д.б.н.;
зам. председателя – Денисова Т.В., доцент каф. РЭТЭМ, к.б.н.

А.А. Данцова, А.П. Шкарупо ВЛИЯНИЕ СЕНОМАНСКИХ РАСТВОРОВ НА РАЗВИТИЕ МОЛЛЮСКОВ	155
---	-----

А.А. Гайворонских ЭКОЛОГИЧЕСКИЕ ПОКАЗАТЕЛИ РЫБ ОЗЕРА ИССЫК-КУЛЬ	157
---	-----

В.И. Иванов ОЦЕНКА ИЗМЕНЕНИЙ БОЛОТНЫХ ЛАНДШАФТОВ ЗАПОВЕДНИКА «ВАСЮГАНСКИЙ» В ПРЕДЕЛАХ ТОМСКОЙ ОБЛАСТИ В ПЕРИОД С 1984 ПО 2016 ГОДЫ.....	159
---	-----

Т.А. Безъязыкова, К.В. Камянецкая ПОЛОЖИТЕЛЬНАЯ ОЦЕНКА СИСТЕМЫ ОХРАНЫ ТРУДА ПРЕДПРИЯТИЯ И ЕЕ АНАЛИЗ	162
--	-----

Е.В. Кандычева ОБЗОР ЛАБОРАТОРНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ С ЦЕЛЮ ВЫЯВЛЕНИЯ КОНКУРЕНТНЫХ ПРЕИМУЩЕСТВ ХИМИЧЕСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ.....	164
--	-----

А.С. Канисеев, Н.С. Симкина РОЛЬ ИЗУЧЕНИЯ МЕР ПОЖАРНОЙ БЕЗОПАСНОСТИ В ПРОЦЕССЕ ПРОФЕССИОНАЛЬНОГО СТАНОВЛЕНИЯ СТУДЕНТОВ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ	167
---	-----

Д.А. Ключева, С.А. Калашиникова ВЛИЯНИЕ НЕФТЕЗАГРЯЗНЕНИЙ НА СООБЩЕСТВА ПОЧВЕННЫХ НЕМАТОД В ЕСТЕСТВЕННЫХ УСЛОВИЯХ	169
---	-----

Т.Е. Лушникова, А.П. Шкарупо ВЛИЯНИЕ БЕНЗИНА НА ПРЕСНОВОДНЫХ РАЧКОВ DAPHNIA MAGNA	171
--	-----

А.С. Мишенева ИССЛЕДОВАНИЕ ПАРАМЕТРОВ МИКРОКЛИМАТА В КОМПЬЮТЕРНЫХ КЛАССАХ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ .	173
--	-----

<i>Е.Р. Моргунова, А.П. Шкарупо</i> ВЛИЯНИЕ БЕНЗИНА НА АКВАРИУМНЫХ РЫБ ROESILIA RETICULATE.....	176
<i>А.А. Мороз, П.В. Тимошенко</i> ИССЛЕДОВАНИЕ ВЛИЯНИЯ СПЕКТРОВ СВЕТА НА РОСТ И РАЗВИТИЕ РАСТЕНИЙ	178
<i>К.И. Мурадян, А.П. Шкарупо</i> ВЛИЯНИЕ НЕФТЕПРОДУКТОВ НА МОЛЛЮСКОВ	181
<i>А.С. Шумилова</i> РАЗРАБОТКА И АПРОБАЦИЯ ЭЛЕКТРОННОГО КУРСА «ОБУЧЕНИЕ ОХРАНЕ ТРУДА»	183
<i>А.А. Тюменцева</i> РАСПРЕДЕЛЕНИЕ ДОЖДЕВЫХ ЧЕРВЕЙ В АНТРОПОГЕННО-НАРУШЕННЫХ ПОЧВАХ	186
<i>Д.А. Коршунова, А.А. Заздравных, Ю.С. Кудрякова, А.О. Ким, Н.А. Конзирович, К.В. Синцев</i> ОПРЕДЕЛЕНИЕ КАЧЕСТВА ВОДЫ В ГЛАВНОМ И УЧЕБНО-ЛАБОРАТОРНОМ КОРПУСАХ ТУСУРА	189
<i>Т.Н. Андреева, А.П. Шкарупо</i> ВЛИЯНИЕ НЕФТЕЗАГРЯЗНЕНИЙ НА УЛИТОК ФИЗА (PHYSA)	189

СЕКЦИЯ 8

POSTGRADUATE AND MASTER STUDENTS' RESEARCH IN ELECTRONICS AND CONTROL SYSTEMS

(Секция на английском языке)

Председатель секции – **Покровская Е.М.**, зав. каф. ИЯ, доцент,
к.филос.н.;

зам. председателя – **Шнит Е.И.**, ст. преподаватель каф. ИЯ;
Соболевская О.В., ст. преподаватель каф. ИЯ

<i>J. Carretero, M. Sargynbayeva</i> SAFETY OF WEARABLE TECHNOLOGY	197
<i>T.E. Grigorieva</i> AUTOMATED INFORMATION MANAGEMENT SYSTEM FOR PLANNING MANAGEMENT DECISIONS ON THE EXAMPLE OF SNOW REMOVAL.....	199
<i>R.R. Khazhibekov</i> ELECTRODYNAMIC SIMULATION OF THE ULTRASHORT PULSE DECOMPOSITION IN THE SEVEN-STAGE MODAL FILTERS LAYOUTS ...	202
<i>V.V. Ignatenko, O.V. Bubnov</i> STATIC RECIPROCAL CONVERTER	205

<i>Z.M. Kurmasheva, F. Videau</i> MACHINE VISION OF THE INMOOV ROBOT	207
<i>A.A. Leshenok, O.A. Lisuro</i> THE STUDIES OF THE MINERAL COMPOSITION OF NATURAL WATERS OF SIBERIA RESORTS.....	210
<i>I.I. Obach, A.A. Abouellail</i> ELECTRICAL NETWORK MONITORING VIA THERMOELECTRICAL COMPONENTS	213
<i>Y.V. Shablya</i> THE CATALAN AND EULER NUMBER TRIANGLES AND THEIR APPLICATION.....	216
<i>R.Yu. Shageev</i> ANALYSIS OF THE DEPENDENCE OF LOSSES ON THE GAP WIDTH BETWEEN WAVEGUIDES OF THE SPOT-SIZE CONVERTER.....	219
<i>A. Zalevskii, R. Vaissié</i> HYBRID VEHICLE FOR FULL AUTONOMY	221
<i>Bouchery Corentin</i> INFORMATION AND COMMUNICATION AREA	224
<i>Florian Guerin</i> THE WELLBEING ENVIRONMENT	226

КРУГЛЫЙ СТОЛ

«ИНТЕГРАЦИЯ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ И РЕСУРСОВ ШКОЛЫ, ТЕХНИКУМА И ВУЗА В ЦЕЛЯХ ПОВЫШЕНИЯ КАЧЕСТВА НЕПРЕРЫВНОЙ ПОДГОТОВКИ СПЕЦИАЛИСТОВ»

<i>В.В. Горовцова</i> МОДЕЛЬ ШКОЛЬНОГО ТЕХНОЛОГИЧЕСКОГО ОБРАЗОВАНИЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ НАПРАВЛЕННОСТИ НА ОСНОВЕ СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ «ШКОЛА – ВУЗ – ПРЕДПРИЯТИЕ» ..	233
<i>Е.Е. Макарова, Ю.В. Храмовских</i> МОДЕЛЬ ШКОЛЬНОГО ТЕХНОЛОГИЧЕСКОГО ОБРАЗОВАНИЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ НАПРАВЛЕННОСТИ НА ОСНОВЕ СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ «ШКОЛА – ВУЗ – ПРЕДПРИЯТИЕ» ...	235
<i>С.А. Калашиникова</i> СТАНОВЛЕНИЕ СИСТЕМЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОГО ОБРАЗОВАНИЯ В АКАДЕМИЧЕСКОМ ЛИЦЕЕ г. ТОМСКА им. Г.А. ПСАХЬЕ.....	237

Научное издание

**Материалы
Международной научно-технической конференции
студентов, аспирантов и молодых ученых
«Научная сессия ТУСУР–2018»**

16–18 мая 2018 г., г. Томск

В пяти частях

Часть 4

Тексты статей даны в авторской редакции, без корректуры
Верстка **В.М. Бочкаревой**

Издательство «В-Спектр».
Сдано на верстку 10.04.2018. Подписано к печати 10.05.2018.
Формат 60×84¹/₁₆. Печать трафаретная. Печ. л. 15,5
Тираж 100 экз. Заказ 11.

Издано ТУСУР, г. Томск, пр. Ленина, 40, к. 205, т. 70-15-24
(записано 700 CD-дисков с электронными версиями всех частей сборника
для нужд всех структурных подразделений университета и авторов)

Издательство «В-Спектр».
634055, г. Томск, пр. Академический, 13-24, т. 49-09-91
E-mail: bvm@sibmail.com