Національний аерокосмічний університет ім. М.Є. Жуковського
«Харківський авіаційний інститут»

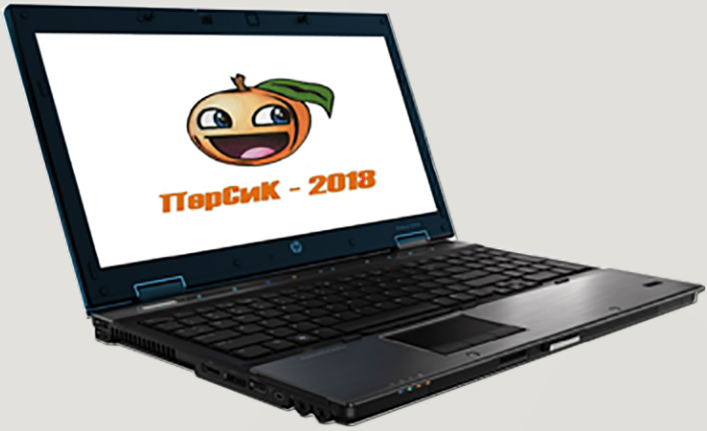
Кафедра комп'ютерних систем, мереж та кібербезпеки

9 науково-технічна конференція студентів

Перспективные Сетевые И Компютерные технологии
Перспективні мережні та комп'ютерні технології
Perspective network and computer technologies

ПерСиК 2018

Матеріали конференції



Україна, Харків, 17 квітня 2018

Министерство образования и науки Украины
Национальный аэрокосмический университет
им. Н.Е. Жуковского «Харьковский авиационный институт»

Кафедра компьютерных систем, сетей и кибербезопасности

совместно с

Аэрокосмическим лицеем на базе ХАИ
Областной специализированной
школой-интернатом «Одаренность»

при поддержке

Проекта ERASMUS+ ALIoT

Научно-техническая конференция

Перспективные сетевые и компьютерные технологии (ПерСиК 2018)

Материалы конференции

Украина, Харьков – 2018

УДК 004
ББК 32.973.2-018+32.844.1

Наведено матеріали тез доповідей за напрямками: комп'ютерні моделі і алгоритми, програмні технології та інструментальні засоби, смарт-системи і мобільні технології, web-, хмарні та технології інтернету речей, кібербезпека.

Рекомендується студентам і магістрам вищих навчальних закладів, які навчаються за спеціальностями напряму «Інформаційні технології», учням старших класів і профільних технікумів, які планують вступати до вищого навчального закладу на дану спеціальність, а також аспірантам, викладачам та науковцям, діяльність яких пов’язана з інформаційними технологіями.

Перспективные сетевые и компьютерные технологии / программа и тезисы докладов 9-й научно-технической конференции «Перспективные сетевые и компьютерные технологии (ПерСиК 2018)», 17 апреля 2018 г. – ФЛП Лысенко И.Б., Харьков, Украина, 2018. – 108 с.

ISBN 978-966-1681-24-7

Приведены материалы тезисов докладов по направлениям: компьютерные модели и алгоритмы, программные технологии и инструментальные средства, смарт-системы и мобильные технологии, web, облачные технологии и интернет вещей, кибербезопасность.

Рекомендуется студентам высших учебных заведений, обучающимся по специальностям направления «Информационные технологии» («Компьютерная инженерия» и «Кибербезопасность»), ученикам старших классов и профильных техникумов, планирующих поступать в университеты на эти специальности, аспирантам, преподавателям и научным работникам, деятельность которых связана с информационными технологиями.

004
32.973.2-018+32.844.1

ISBN 978-966-1681-24-7

СОДЕРЖАНИЕ

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ 12

ПЛАН КОНФЕРЕНЦИИ..... 13

ПРОГРАММА КОНФЕРЕНЦИИ 14

ТЕЗИСЫ ДОКЛАДОВ 24

Borbytska V.K.
RED-BLACK TREES: IMPLEMENTATION, MODELLING AND EFFECTIVENESS RESEARCH..... 24

Nzabahimana Jean Pierre
VENDOR DIVERSITY DEPLOYMENT IN IOT TO PROVIDE A HIGH AVAILABILITY..... 25

Смидович Л.Л.
ИНСТРУМЕНТАЛЬНОЕ СРЕДСТВО СРАВНЕНИЯ АЛГОРИТМОВ СОРТИРОВКИ 26

Ouafa Dahibi
SYSTEM OF QUADCOPTER 27

Labatt M.A.
INTERNET OF THINGS: HEALTHCARE AND MEDICINE..... 28

Сверчков Д.А.
РАЗРАБОТКА УСТРОЙСТВА ДЛЯ АВТОМАТИЧЕСКОГО ПОЗИЦИОНИРОВАНИЯ ПАНЕЛЕЙ СОЛНЕЧНЫХ БАТАРЕЙ..... 29

Parfenova I.V.
INVESTIGATION OF THE SHAPE OF AN ULTRASONIC SIGNAL REFLECTED BY AN UNEVEN SURFACE 30

Dube Mandlaenkosi. B
LIGHTS IN AVIATION – THEIR USES.....31

Ben Hassen Jehan
AIRBORNE WEATHER RADAR 32

Salahdine Khiarhoum
RELIABILITY ASSESSMENT OF INTERNET OF THINGS IN SMART HOME 33

Tavrin A.V.
WORK AUTOMATION IN SALES DEPARTMENT.....34

Федько А.Д.
ДИНАМИЧЕСКАЯ ФОНОВАЯ ПОДСВЕТКА ЭКРАНА МОНИТОРА НА ARDUINO NANO.....35

Alanamu M.A.
THREAT MITIGATION FOR OPENSTACK CLOUD: DRIVERS AND STOPPERS 36

Bansi Parsania
COLONIZATION ON MARS 37

Demidenko D.V.
AUTOMATION OF TECHNOLOGICAL PROCESSES IN MANUFACTURING INTERNET OF THINGS CONTEXT FOR PHARMACEUTICAL ENTERPRISES.....38

Peñaloza G.S.
DEVELOPMENT OF LANGUAGE LEARNING TOOL 39

Поповиченко О.Н.
РАЗРАБОТКА СРЕДСТВА КОНТРОЛЯ ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ РАБОЧЕГО ВРЕМЕНИ 40

Титаренко В.С.
АНАЛИЗ АЛГОРИТМОВ ЭВРИСТИЧЕСКОГО ПОИСКА.....41

Лаврик И.С.
АКТУАЛЬНОСТЬ И ПРОБЛЕМАТИКА ПРАКТИЧЕСКОГО ИСПОЛЬЗОВАНИЯ ЦИФРОВОГО ЗВУКА И DAW.....42

Герус В.А.
ЗАДАЧА О РЮКЗАКЕ 43

Казаков Г.С., Тимошевський Д.С.
ПРОГРАМНА РЕАЛІЗАЦІЯ АЛГОРИТМУ РОЗПІЗНАВАННЯ ФІЗИЧНИХ СХЕМ ТА ПОКАЗНИКІВ ФІЗИЧНИХ АНАЛОГОВИХ ПРИБОРІВ У РЕАЛЬНОМУ ЧАСІ «RECOON».....44

Лаптев А.А.
РАЗРАБОТКА ПРОГРАММЫ ДЛЯ ИЗУЧЕНИЯ ОСНОВ КРИПТОГРАФИИ C.G.LEARN.....45

Лаптий А.А.
ОСОБЕННОСТИ РАЗРАБОТКИ РПГ-ИГР В СРЕДЕ РАЗРАБОТКИ RPG MAKER.....46

Белоус Н.К.
ИГРОВАЯ ЗАДАЧА «ЦЗЯНЬШИДЗЫ».....47

Сидоренко Ю.А.
ИГРОВАЯ ЗАДАЧА «ХАНОЙСКАЯ БАШНЯ».....48

Таланцев М.Є.
ВЛАСНА ПРОГРАМНА РЕАЛІЗАЦІЯ АЛГОРИТМУ АСИМЕТРИЧНОГО ШИФРУВАННЯ NTRU.....49

Кузін А.В.
ОРГАНІЗАЦІЯ АРИФМЕТИКО ЛОГІЧНОГО ПРИСТРОЮ КОМП'ЮТЕРА.....50

Кирьян Е.П.
ОБУЧЕНИЕ ПЕРЕВОДУ В РАЗЛИЧНЫЕ СИСТЕМЫ СЧИСЛЕНИЯ.....51

Хмелевцова М.А.
ОБУЧЕНИЕ ПЕРЕВОДУ В РАСПРОСТРАНЕННЫЕ СИСТЕМЫ СЧИСЛЕНИЯ.....52

Гладкова А.О.
ПРОГРАМНИЙ КОДЕР/ДЕКОДЕР ПАКЕТІВ ІНФОРМАЦІЇ З CRC15 ЗАХИСТУ ТЕКСТОВИХ ФАЙЛІВ.....53

Зиноватный М.А.
РАЗРАБОТКА ПРИЛОЖЕНИЯ ДЛЯ АВТОМАТИЗАЦИИ И ИССЛЕДОВАНИЯ МЕТОДОВ ИЗМЕРЕНИЯ ВИБРАЦИЙ ПЕЧАТНЫХ УЗЛОВ РАДЕОЭЛЕКТРОННОЙ АППРАТУРЫ 54

Шевяк К.И.
АНИМАЦИЯ В WPF.....55

Третьякова Ю.Ю.
ИССЛЕДОВАНИЕ КЛЕТОЧНЫХ АВТОМАТОВ НА ПРИМЕРЕ ИГРЫ "ЖИЗНЬ".....56

Нгуен А.В., Сидоров Я.Е.
ОЦЕНКА ЭФФЕКТИВНОСТИ РАБОТЫ КАПСУЛЬНОЙ АРХИТЕКТУРЫ НЕЙРОННЫХ СЕТЕЙ В СРАВНЕНИИ СО СВЕРТОЧНОЙ АРХИТЕКТУРОЙ 57

Андриенко А.И.
РАЗРАБОТКА КЛАССА АВЛ-ДЕРЕВА 58

Тимохин И.С.
РЕАЛИЗАЦИЯ ОПЕРАЦИЙ С БИНАРНЫМИ ДЕРЕВЬЯМИ И ОЦЕНКА ИХ БЫСТРОДЕЙСТВИЯ.....59

Кошель М.А.
СРАВНЕНИЕ АЛГОРИТМОВ СОРТИРОВКИ 60

Лукьяненко К.С.
СРАВНЕНИЕ СИММЕТРИЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ.....61

Третяк І.Р.
ПРОГРАМНЕ ДОДАВАННЯ ЛАНЦЮГІВ ПАКЕТУ БАЙТІВ ЧИСЕЛ ЗІ ЗНАКОМ.....62

Шулінус О.А.
КОМП'ЮТЕРНИЙ МОНІТОРИНГ ПРОГРАМНОЇ ЕМУЛЯЦІЇ ДОДАВАННЯ РЕАЛЬНИХ ЧИСЕЛ ПОДВІЙНОЇ ТОЧНОСТІ 63

Сушинський В.В.
МНОГОПОТОЧНОСТЬ В WPF.....64

Судаков Д.А.
ПРОГРАММА ДЛЯ ПОСТРОЕНИЕ ГРАФИКОВ ФУНКЦИЙ 65

Шорский А.Э.
ПОСТРОЕНИЕ ЛАБИРИНТОВ С ПОМОЩЬЮ АЛГОРИТМА ЭЛЛЕРА.....66

Цокота Я.В.
РАЗРАБОТКА ОЧЕРЕДИ С ПРИОРИТЕТОМ 67

Саєнко В.А.
ДОСЛІДЖЕННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ РОБОТИ РЕЛЯЦІЙНИХ ТА НЕРЕЛЯЦІЙНИХ БАЗ ДАНИХ НА ПРИКЛАДІ MS SQL SERVER ТА MONGO DB 68

Кальницкий М.Э.
РАЗРАБОТКА И ИССЛЕДОВАНИЕ МЕТОДИКИ ОЦЕНИВАНИЯ КАЧЕСТВА СИСТЕМ ОТСЛЕЖИВАНИЯ ОШИБОК 69

Тихонов А.В.
РАСПРЕДЕЛЕННАЯ СИСТЕМА МОНИТОРИНГА НА ОСНОВЕ БПЛА.....70

Medvediev I.A.
IOT SOLUTIONS FOR HEALTH MONITORING: ANALYSIS AND CASE STUDY.....71

Косаревский Б.В.
АНАЛИЗ ВАРИАНТОВ МАРШРУТИЗАЦИИ УПРАВЛЯЮЩИХ СИГНАЛОВ В БЕСПРОВОДНЫХ СЕТЯХ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ УПРАВЛЕНИЯ ИСПОЛНИТЕЛЬНЫМИ УСТРОЙСТВАМИ УМНОГО ДОМА.....72

Землянко Г.А.
РАЗРАБОТКА ПРИЛОЖЕНИЯ БЕСПРОВОДНОГО УПРАВЛЕНИЯ СВЕТОДИОДНОЙ ЛЕНТОЙ С ПИКСЕЛЬНОЙ АДРЕСАЦИЕЙ.....73

Хебнев А.В.
РАЗРАБОТКА МОДУЛЯ БЕСПРОВОДНОГО УПРАВЛЕНИЯ СВЕТОДИОДНОЙ ЛЕНТОЙ С ПИКСЕЛЬНОЙ АДРЕСАЦИЕЙ 74

Бєлінський Р.А.
ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ РОЗВИТКУ МОБІЛЬНОГО ІНТЕРНЕТУ ПОКОЛІННЯ 3G. РОЗРОБКА ВЛАСНОЇ ПРОГРАМИ «BNG» ДЛЯ КРАЩОГО ПОШИРЕННЯ СИГНАЛУ ..75

Новоспасский А.С.
ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ТЕХНОЛОГИИ INTERNET OF THINGS.....76

Товкало Е.П., Хапокныш Ю.В.
ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ БЕСПИЛОТНЫХ АППАРАТОВ 77

Чуйко А.А., Гулий В.В.
МОНИТОРИНГ С ИСПОЛЬЗОВАНИЕМ КВАДРОКОПТЕРОВ В СОСТАВЕ ПРОЕКТА SMART CITY .78

Москаленко Б.В.
АНАЛИЗ ПРОГРАММНЫХ СРЕДСТВ ПОВЫШЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ КЛИЕНТСКОЙ ЧАСТИ WEB-ПРИЛОЖЕНИЙ.....79

Нос Р.С.
МОДЕЛЬ КРИПТОПРЕОБРАЗОВАНИЯ ДАННЫХ ПО СХЕМЕ ЗАДАЧИ О РЮКЗАКЕ НА ОСНОВЕ ПРИНЦИПА ДИВЕРСНОСТИ 80

Почернин А.М.
РАЗРАБОТКА И ИССЛЕДОВАНИЕ ИНСТРУМЕНТАЛЬНОГО СРЕДСТВА ДЛЯ ОЦЕНКИ СТАРТАП-ПРОЕКТОВ. 81

Андрийчук А.С.
ИССЛЕДОВАНИЕ И РАЗРАБОТКА МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ В КОНТЕКСТЕ ЗДРАВООХРАНЕНИЯ 82

Павлюков Е.А.
RFID СКУД С ИСПОЛЬЗОВАНИЕМ СЕТЕВЫХ ТЕХНОЛОГИЙ 83

Геллер С.И.
АНАЛИЗ ДОРОЖНОЙ ОБСТАНОВКИ И ОЦЕНКА ОПАСНОСТИ НА ДОРОГЕ 84

Карпенко А.С.
РЕАЛИЗАЦИЯ ПРОТОКОЛА УПРАВЛЕНИЯ ЭЛЕКТРОННЫМ КЛЮЧЕМ ПО БЕСПРОВОДНОМУ КАНАЛУ СВЯЗИ 85

Карпенко А.С.
АНАЛИЗ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ ТЕХНОЛОГИЙ 86

Карпенко А.С.
АНАЛИЗ STATELESS СХЕМ ЦИФРОВОЙ ПОДПИСИ С УЧЕТОМ КВАНТОВОЙ ЗАЩИЩЕННОСТИ 87

Бородавка В.В.
БІОМЕТРИЧНІ СИСТЕМИ ЯК ЗАСІБ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ 88

Трегуб Ю.В.
ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ ВІД КІБЕРЗЛОЧИНЦІВ 89

Дука И.А.
АЛГОРИТМ ШИФРОВАНИЯ «КУЗНЕЧИК» И СРАВНЕНИЕ ЕГО С ДРУГИМИ СТАНДАРТАМИ БСШ 90

Кийко О.Д.
ЧАСТОТНЫЙ СЛОВАРЬ.....91

Фролов А.В., Фролов В.В.
ПОСТ-КВАНТОВЫЕ АЛГОРИТМЫ ЦИФРОВОЙ ПОДПИСИ ОСНОВАННЫЕ НА ХЕШ-ФУНКЦИЯХ.....92

Гвоздинский М. А.
ПОДХОД К ФОРМИРОВАНИЮ РАСПИСАНИЯ КЛЮЧЕЙ ДЛЯ БЛОЧНОГО СИММЕТРИЧНОГО КРИПТОАЛГОРИТМА ГОСТ 28147-89.....93

Брошеван Е.В.
АНАЛИЗ ТЕХНОЛОГИИ EDELIVERY В КОНТЕКСТЕ ПРЕДОСТАВЛЕНИЯ ЭЛЕКТРОННЫХ ДОВЕРИТЕЛЬНЫХ УСЛУГ.....94

Марченко А.О.
АНАЛИЗ МЕТОДОЛОГИЙ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ.....95

Скрябин Н.К.
ПРОГРАММНОЕ СРЕДСТВО ДЛЯ ВЫЯВЛЕНИЯ ВИРУСОВ-МАЙНЕРОВ В ЛОКАЛЬНОЙ СЕТИ.....96

Вешкин Д.А.
МОДЕЛЬ КРИПТОПРЕОБРАЗОВАНИЯ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ГЕНЕТИЧЕСКОГО АЛГОРИТМА НА ОСНОВЕ ПРИНЦИПА ДИВЕРСНОСТИ 97

Радченко Н.В.
ИССЛЕДОВАНИЕ МЕТОДА ПОСТРОЕНИЯ ПРОСТЫХ ЧИСЕЛ 98

Yasko A.V.
CONSIDERING EXPERT UNCERTAINTY DURING SAFETY ASSESSMENT OF FPGA-BASED NPP I&C SYSTEMS..... 99

Войков Ю.В.
РАЗРАБОТКА СЧИТЫВАТЕЛЯ БЕСКОНТАКТНЫХ КАРТ 100

Власов Ю.А.
СРЕДСТВА ПРОТОТИПИРОВАНИЯ ДЛЯ IOT СИСТЕМ ОСНОВАННЫХ НА ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ 101

Годованюк П.А.
АНАЛИЗ ТЕХНОЛОГИИ SDN SECURITY 102

АЛФАВИТНЫЙ УКАЗАТЕЛЬ 103

ДЛЯ ЗАМЕТОК 105

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ

Харченко Вячеслав Сергеевич, заслуженный изобретатель Украины, доктор технических наук, профессор, заведующий кафедрой компьютерных систем, сетей и кибербезопасности ХАИ – председатель;

Перепелицын Артем Евгеньевич, ст. преподаватель;

Nzabahimana Jean Pierre, студент 6-го курса;

Титаренко Владислава Сергеевна, студентка 2-го курса;

Третьякова Юлия Юрьевна, студентка 2-го курса;

Шевяк Кирилл Игоревич, студент 2-го курса;

ПРОГРАММНЫЙ КОМИТЕТ

Перепелицын Артем Евгеньевич, ст. преподаватель – председатель;

Лысенко Игорь Владимирович, к.т.н., доцент;

Вамболь Алексей Сергеевич, аспирант.

ПЛАН КОНФЕРЕНЦИИ

17 апреля 2018 г. Время: 13:30 – 19:00, радиокорпус ХАИ

13:30 – 14:00	**РЕГИСТРАЦИЯ УЧАСТНИКОВ**				
14:00 – 15:00	**Пленарное заседание, ауд. 233**				
	Секция 1,ауд. 233	**Секция 2, ауд. 132**	**Секция 3, ауд. 123**	**Секция 4, ауд. 136в**	**Секция 5, ауд. 229**
	Смарт-системы и мобильные технологии	Программные технологии и инструментальные средства	Компьютерные модели и алгоритмы	Web, облачные технологии и Интернет вещей	Кибербезопасность и криптозащита
	Smart systems and mobile technologies	Software technologies and tools	Models and algorithms of computing	Web, Cloud computing and IOTs	Cybersecurity and cryptography
15:05 – 16:45	Сессия 1.1	Сессия 2.1	Сессия 3.1	Сессия 4.1	Сессия 5.1
16:45 – 17:00	**КОФЕ-БРЕЙК**				
17:00 – 18:35	Сессия 1.2	Сессия 2.2	Сессия 3.2	Сессия 4.2	Сессия 5.2
18:45 – 19:00	**Итоговое пленарное заседание, ауд. 233**				

ПРОГРАММА КОНФЕРЕНЦИИ

---

17 апреля 2018 г.

Пленарное заседание, ауд. 233, радиокорпус ХАИ, 14:00-15:00

Открытие конференции

Приветствие участников

Пленарный доклад:
д.т.н., проф., СНУ ім. В. Даля, Сєвєродонецьк,
Скарга-Бандурова І.С.
Deep Learning: Можливості, Обрії та Кордони

Секция 1, ауд. 233, 15.05 – 18.35
Смарт-системы и мобильные технологии

Модератор: ст. преподаватель Перепелицын А.Е.
Сомодератор: студент Nzabahimana Jean Pierre

Сессия 1.1

Borbytska V.K.
RED-BLACK TREES: IMPLEMENTATION, MODELLING AND EFFECTIVENESS RESEARCH

Nzabahimana Jean Pierre
VENDOR DIVERSITY DEPLOYMENT IN IOT TO PROVIDE A HIGH AVAILABILITY

Смидович Л.Л.
ИНСТРУМЕНТАЛЬНОЕ СРЕДСТВО СРАВНЕНИЯ АЛГОРИТМОВ СОРТИРОВКИ

Ouafa Dahibi
SYSTEM OF QUADCOPTER

Labatt M.A.
INTERNET OF THINGS: HEALTHCARE AND MEDICINE

Сверчков Д.А.
РАЗРАБОТКА УСТРОЙСТВА ДЛЯ АВТОМАТИЧЕСКОГО ПОЗИЦИОНИРОВАНИЯ ПАНЕЛЕЙ СОЛНЕЧНЫХ БАТАРЕЙ

Parfenova I.V.
INVESTIGATION OF THE SHAPE OF AN ULTRASONIC SIGNAL REFLECTED BY AN UNEVEN SURFACE

Dube Mandlaenkosi. B
LIGHTS IN AVIATION – THEIR USES

Сессия 1.2

Ben Hassen Jehan
AIRBORNE WEATHER RADAR

Salahdine Khiarhoum
RELIABILITY ASSESSMENT OF INTERNET OF THINGS IN SMART HOME

Tavrin A.V.
WORK AUTOMATION IN SALES DEPARTMENT

Федько А.Д.
ДИНАМИЧЕСКАЯ ФОНОВАЯ ПОДСВЕТКА ЭКРАНА МОНИТОРА НА ARDUINO NANO

Alanamu M.A.
THREAT MITIGATION FOR OPENSTACK CLOUD: DRIVERS AND STOPPERS

Bansi Parsania
COLONIZATION ON MARS

Demidenko D.V.
AUTOMATION OF TECHNOLOGICAL PROCESSES
IN MANUFACTURING INTERNET OF THINGS CONTEXT
FOR PHARMACEUTICAL ENTERPRISES

Peñaloza G.S.
DEVELOPMENT OF LANGUAGE LEARNING TOOL

Секция 2, ауд. 132, 15.05 – 18.35
Программные технологии и инструментальные средства

Модератор: ассистент Егорова Е.В.
Сомодератор: студент Войков Ю.В.

Сессия 2.1

Поповиченко О.Н.
РАЗРАБОТКА СРЕДСТВА КОНТРОЛЯ ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ РАБОЧЕГО ВРЕМЕНИ

Титаренко В.С.
АНАЛИЗ АЛГОРИТМОВ ЭВРИСТИЧЕСКОГО ПОИСКА

Лаврик И.С.
АКТУАЛЬНОСТЬ И ПРОБЛЕМАТИКА ПРАКТИЧЕСКОГО ИСПОЛЬЗОВАНИЯ ЦИФРОВОГО ЗВУКА И DAW

Герус В.А.
ЗАДАЧА О РЮКЗАКЕ

Казаков Г.С., Тимошевський Д.С.
ПРОГРАМНА РЕАЛІЗАЦІЯ АЛГОРИТМУ РОЗПІЗНАВАННЯ ФІЗИЧНИХ СХЕМ ТА ПОКАЗНИКІВ ФІЗИЧНИХ АНАЛОГОВИХ ПРИБОРІВ У РЕАЛЬНОМУ ЧАСІ «RECOON»

Лаптев А.А.
РАЗРАБОТКА ПРОГРАММЫ ДЛЯ ИЗУЧЕНИЯ
ОСНОВ КРИПТОГРАФИИ C.G.LEARN

Лаптий А.А.
ОСОБЕННОСТИ РАЗРАБОТКИ РПГ-ИГР
В СРЕДЕ РАЗРАБОТКИ RPG MAKER

Сессия 2.2

Белоус Н.К.
ИГРОВАЯ ЗАДАЧА «ЦЗЯНЬШИДЗЫ»

Сидоренко Ю.А.
ИГРОВАЯ ЗАДАЧА «ХАНОЙСКАЯ БАШНЯ»

Таланцев М.Є.
ВЛАСНА ПРОГРАМНА РЕАЛІЗАЦІЯ АЛГОРИТМУ
АСИМЕТРИЧНОГО ШИФРУВАННЯ NTRU

Кузін А.В.
ОРГАНІЗАЦІЯ АРИФМЕТИКО ЛОГІЧНОГО
ПРИСТРОЮ КОМП'ЮТЕРА

Кирьян Е.П.
ОБУЧЕНИЕ ПЕРЕВОДУ В РАЗЛИЧНЫЕ
СИСТЕМЫ СЧИСЛЕНИЯ

Хмелевцова М.А.
ОБУЧЕНИЕ ПЕРЕВОДУ В РАСПРОСТРАНЕННЫЕ
СИСТЕМЫ СЧИСЛЕНИЯ

Гладкова А.О.
ПРОГРАМНИЙ КОДЕР/ДЕКОДЕР ПАКЕТІВ ІНФОРМАЦІЇ
З CRC15 ЗАХИСТУ ТЕКСТОВИХ ФАЙЛІВ

Зиноватный М.А.
РАЗРАБОТКА ПРИЛОЖЕНИЯ ДЛЯ АВТОМАТИЗАЦИИ И ИССЛЕДОВАНИЯ МЕТОДОВ ИЗМЕРЕНИЯ ВИБРАЦИЙ ПЕЧАТНЫХ УЗЛОВ РАДЕОЭЛЕКТРОННОЙ АППРАТУРЫ

Секция 3, ауд. 123, 15.05 – 18.35
Компьютерные модели и алгоритмы

Модератор: аспирант Мерлак В.Ю.
Сомодератор: студент Власов Ю.А.

Сессия 3.1

Шевяк К.И.
АНИМАЦИЯ В WPF

Третьякова Ю.Ю.
ИССЛЕДОВАНИЕ КЛЕТОЧНЫХ АВТОМАТОВ
НА ПРИМЕРЕ ИГРЫ "ЖИЗНЬ"

Нгуен А.В., Сидоров Я.Е.
ОЦЕНКА ЭФФЕКТИВНОСТИ РАБОТЫ КАПСУЛЬНОЙ АРХИТЕКТУРЫ НЕЙРОННЫХ СЕТЕЙ В СРАВНЕНИИ СО СВЕРТОЧНОЙ АРХИТЕКТУРОЙ

Андриенко А.И.
РАЗРАБОТКА КЛАССА АВЛ-ДЕРЕВА

Тимохин И.С.
РЕАЛИЗАЦИЯ ОПЕРАЦИЙ С БИНАРНЫМИ ДЕРЕВЬЯМИ И ОЦЕНКА ИХ БЫСТРОДЕЙСТВИЯ

Кошель М.А.
СРАВНЕНИЕ АЛГОРИТМОВ СОРТИРОВКИ

Лукьяненко К.С.
СРАВНЕНИЕ СИММЕТРИЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ

Сессия 3.2

Третяк І.Р.
ПРОГРАМНЕ ДОДАВАННЯ ЛАНЦЮГІВ ПАКЕТУ БАЙТІВ ЧИСЕЛ ЗІ ЗНАКОМ

Шулінус О.А.
КОМП'ЮТЕРНИЙ МОНІТОРИНГ ПРОГРАМНОЇ ЕМУЛЯЦІЇ ДОДАВАННЯ РЕАЛЬНИХ ЧИСЕЛ ПОДВІЙНОЇ ТОЧНОСТІ

Сушинський В.В.
МНОГОПОТОЧНОСТЬ В WPF

Судаков Д.А.
ПРОГРАММА ДЛЯ ПОСТРОЕНИЕ ГРАФИКОВ ФУНКЦИЙ

Шорский А.Э.
ПОСТРОЕНИЕ ЛАБИРИНТОВ С ПОМОЩЬЮ АЛГОРИТМА ЭЛЛЕРА

Цокота Я.В.
РАЗРАБОТКА ОЧЕРЕДИ С ПРИОРИТЕТОМ

Саєнко В.А.
ДОСЛІДЖЕННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ РОБОТИ РЕЛЯЦІЙНИХ ТА НЕРЕЛЯЦІЙНИХ БАЗ ДАНИХ НА ПРИКЛАДІ MS SQL SERVER ТА MONGO DB

Кальницкий М.Э.
РАЗРАБОТКА И ИССЛЕДОВАНИЕ МЕТОДИКИ ОЦЕНИВАНИЯ КАЧЕСТВА СИСТЕМ ОТСЛЕЖИВАНИЯ ОШИБОК

Рева М.В.
МОНІТОРИНГ АРИФМЕТИЧНИХ ПРАПОРІВ ОБЧИСЛЮВАЛЬНОГО ЯДРА КОМП'ЮТЕРА

Секция 4, ауд. 136в, 15.05 – 18.35
Web, облачные технологии и Интернет вещей

Модератор: ассистент Тецкий А.Г.
Сомодератор: студент Медведев И.А.

Сессия 4.1

Тихонов А.В.
РАСПРЕДЕЛЕННАЯ СИСТЕМА МОНИТОРИНГА
НА ОСНОВЕ БПЛА

Medvediev I.A.
IOT SOLUTIONS FOR HEALTH MONITORING:
ANALYSIS AND CASE STUDY

Косаревский Б.В.
АНАЛИЗ ВАРИАНТОВ МАРШРУТИЗАЦИИ
УПРАВЛЯЮЩИХ СИГНАЛОВ В БЕСПРОВОДНЫХ
СЕТЯХ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ УПРАВЛЕНИЯ
ИСПОЛНИТЕЛЬНЫМИ УСТРОЙСТВАМИ УМНОГО ДОМА

Землянко Г.А.
РАЗРАБОТКА ПРИЛОЖЕНИЯ БЕСПРОВОДНОГО
УПРАВЛЕНИЯ СВЕТОДИОДНОЙ ЛЕНТОЙ
С ПИКСЕЛЬНОЙ АДРЕСАЦИЕЙ

Хебнев А.В.
РАЗРАБОТКА МОДУЛЯ БЕСПРОВОДНОГО
УПРАВЛЕНИЯ СВЕТОДИОДНОЙ ЛЕНТОЙ
С ПИКСЕЛЬНОЙ АДРЕСАЦИЕЙ

Бєлінський Р.А.
ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ РОЗВИТКУ
МОБІЛЬНОГО ІНТЕРНЕТУ ПОКОЛІННЯ 3G.
РОЗРОБКА ВЛАСНОЇ ПРОГРАМИ «BNG»
ДЛЯ КРАЩОГО ПОШИРЕННЯ СИГНАЛУ

Новоспасский А.С.
ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ТЕХНОЛОГИИ
INTERNET OF THINGS

Товкало Е.П., Хапокныш Ю.В.
ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ
БЕСПИЛОТНЫХ АППАРАТОВ

Сессия 4.2

Чуйко А.А., Гулий В.В.
МОНИТОРИНГ С ИСПОЛЬЗОВАНИЕМ
КВАДРОКОПТЕРОВ В СОСТАВЕ ПРОЕКТА SMART CITY

Москаленко Б.В.
АНАЛИЗ ПРОГРАММНЫХ СРЕДСТВ ПОВЫШЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ КЛИЕНТСКОЙ ЧАСТИ
WEB-ПРИЛОЖЕНИЙ

Нос Р.С.
МОДЕЛЬ КРИПТОПРЕОБРАЗОВАНИЯ ДАННЫХ
ПО СХЕМЕ ЗАДАЧИ О РЮКЗАКЕ
НА ОСНОВЕ ПРИНЦИПА ДИВЕРСНОСТИ

Почернин А.М.
РАЗРАБОТКА И ИССЛЕДОВАНИЕ ИНСТРУМЕНТАЛЬНОГО СРЕДСТВА ДЛЯ ОЦЕНКИ СТАРТАП-ПРОЕКТОВ

Андрийчук А.С.
ИССЛЕДОВАНИЕ И РАЗРАБОТКА МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ В КОНТЕКСТЕ ЗДРАВООХРАНЕНИЯ

Павлюков Е.А.
RFID СКУД С ИСПОЛЬЗОВАНИЕМ
СЕТЕВЫХ ТЕХНОЛОГИЙ

Геллер С.И.
АНАЛИЗ ДОРОЖНОЙ ОБСТАНОВКИ
И ОЦЕНКА ОПАСНОСТИ НА ДОРОГЕ

Секция 5, ауд. 229, 15.05 – 18.35
Кибербезопасность и криптозащита

Модератор: ст. преподаватель Цуранов М.В.
Сомодератор: студент Годованюк П.А.

Сессия 5.1

Карпенко А.С.
РЕАЛИЗАЦИЯ ПРОТОКОЛА УПРАВЛЕНИЯ
ЭЛЕКТРОННЫМ КЛЮЧЕМ
ПО БЕСПРОВОДНОМУ КАНАЛУ СВЯЗИ

Карпенко А.С.
АНАЛИЗ БЕЗОПАСНОСТИ
БЕСПРОВОДНЫХ ТЕХНОЛОГИЙ

Карпенко А.С.
АНАЛИЗ STATELESS СХЕМ ЦИФРОВОЙ ПОДПИСИ
С УЧЕТОМ КВАНТОВОЙ ЗАЩИЩЕННОСТИ

Бородавка В.В.
БІОМЕТРИЧНІ СИСТЕМИ
ЯК ЗАСІБ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ

Трегуб Ю.В.
ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ЗАХИСТУ
ІНФОРМАЦІЙНИХ СИСТЕМ ВІД КІБЕРЗЛОЧИНЦІВ

Дука И.А.
АЛГОРИТМ ШИФРОВАНИЯ «КУЗНЕЧИК»
И СРАВНЕНИЕ ЕГО С ДРУГИМИ СТАНДАРТАМИ БСШ

Кийко О.Д.
ЧАСТОТНЫЙ СЛОВАРЬ

Фролов А.В., Фролов В.В.
ПОСТ-КВАНТОВЫЕ АЛГОРИТМЫ ЦИФРОВОЙ
ПОДПИСИ ОСНОВАННЫЕ НА ХЕШ-ФУНКЦИЯХ

Сессия 5.2

Гвоздинский М. А.
ПОДХОД К ФОРМИРОВАНИЮ РАСПИСАНИЯ КЛЮЧЕЙ ДЛЯ БЛОЧНОГО СИММЕТРИЧНОГО КРИПТОАЛГОРИТМА ГОСТ 28147-89

Брошеван Е.В.
АНАЛИЗ ТЕХНОЛОГИИ EDELIVERY В КОНТЕКСТЕ ПРЕДОСТАВЛЕНИЯ ЭЛЕКТРОННЫХ ДОВЕРИТЕЛЬНЫХ УСЛУГ

Марченко А.О.
АНАЛИЗ МЕТОДОЛОГИЙ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

Скрябин Н.К.
ПРОГРАММНОЕ СРЕДСТВО ДЛЯ ВЫЯВЛЕНИЯ ВИРУСОВ-МАЙНЕРОВ В ЛОКАЛЬНОЙ СЕТИ

Вешкин Д.А.
МОДЕЛЬ КРИПТОПРЕОБРАЗОВАНИЯ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ГЕНЕТИЧЕСКОГО АЛГОРИТМА НА ОСНОВЕ ПРИНЦИПА ДИВЕРСНОСТИ

Радченко Н.В.
ИССЛЕДОВАНИЕ МЕТОДА ПОСТРОЕНИЯ ПРОСТЫХ ЧИСЕЛ

Итоговое пленарное заседание, ауд. 233, 18:45 – 19:00

Выступление руководителей секций

Награды за лучшие доклады

Закрытие конференции

UDC 004.043

RED-BLACK TREES: IMPLEMENTATION, MODELLING AND EFFECTIVENESS RESEARCH

Borbytska V.K., Student of group 525,
Scientific advisor Anatoly Shostak,
National Aerospace University named after N.E. Zhukovsky "KhAI"

As the saying goes, time is what we want most, but what we use worst. It is greatly important for us to facilitate our lives and therefore we have to find the best solutions to all the problems we encounter. What do we look for when we think of the ways to improve our life for better? For effectiveness and performance. Constant development is the law of life, and taking this into account, it is extremely important to work on the effectiveness and performance to save our time.

Due to increasing complexity of today's information systems, special techniques are needed for the best efficiency acquirement. There are a lot of data structures and all of them differ in their complexity. Clearly, it is necessary to understand already existing solutions in order to propose new ones that consider ancestors faults.

The goal of our research is to implement Red-Black Tree structure and compare it with other types of structures. This allows us to find the situations where Red-Black Tree structure can be used in the most efficient way.

Gained results show that specific data structures should be chosen based on expected patterns in the input and the mix of operations to be performed. Memory consumption, time it took to create and lookup time comparisons point out that even though Red-Black Tree is a good example of a powerful structure, it can be outperformed by Hash Tables and AVL-Trees. Still, Red-Black Trees are more efficient than Arrays, Linked Lists, Queues and Stacks.

Hence, we have to understand that no specific data structure on its own is a panacea, and the only key solution is to continue improving existing data structures by picking advantages from each one and combining it with others.

UDC 004.052

VENDOR DIVERSITY DEPLOYMENT IN IoT TO PROVIDE A HIGH AVAILABILITY

Jean Pierre Nzabahimana, Student of group 565FJ,
Scientific advisor Vitaliy Kulanov,
National Aerospace University named after N.E. Zhukovsky "KhAI"

Introduction. we are in a digital world, thousands of objects are being connected every day, sharing information, processing data and accomplishing a specific task without the need of human intervention. Those objects can be connected machine to machine or machine to human. The number of those connected objects will reach 80 billion by the year of 2025, i.e. the internet of things. There are many critical systems where IoT plays a tremendous role; among them Healthcare is number one. When it comes to healthcare systems, availability must be five nines, it means we must minimize downtime so that the system will always be up and running. That will be achieved by applying different methods of redundancy system.

Motivation. failures in IoT systems can be a catastrophe.it can even cost the lives of people, economic crisis may take place, company may lose the trust from its customers. especially when it comes to healthcare. by applying vendor diversity, the availability will be higher because the probability of having failures in two systems from different vendors is very low.

Goal. the goal of this research is to provide a high availability in IoT systems by removing a single point of failure. this will be achieved by deploying a redundancy system that will use duplicated ISP, Firewalls, WAP.

Results. After analyzing the block diagram of vendor diversity in IoT, there will be a high availability in different critical systems such as healthcare, if one component fails, another one will take over immediately so that the system will stay up and running the downside of this model is a high cost. depending on how critical IoT is, this model of vendor diversity can be deployed or not.

УДК 004.424:510.52

ИНСТРУМЕНТАЛЬНОЕ СРЕДСТВО СРАВНЕНИЯ АЛГОРИТМОВ СОРТИРОВКИ

Смидович Л.Л., студент 525 гр.,
Научный руководитель: доцент Шостак А.В.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

В эпоху компьютерных и информационных технологий, особо остро стоит вопрос экономии времени. Экономия даже одной миллисекунды в больших масштабах даст значимую оптимизацию, чтобы оправдать приложенные усилия. Мир не стоит на месте, растут мощности и потребности, и их нужно оптимизировать, ведь время самый ограниченный ресурс.

Человеку проще воспринимать упорядоченный материал, поэтому сортировка является важным элементом информационных технологий. Существует множество алгоритмов сортировки. Каждые из них имеют свою эффективность, слабые и сильные стороны. Для того, чтобы оптимизировать процесс сортировки, необходимо понять, в каких ситуациях какой алгоритм лучше использовать (с учётом масштаба и условий задачи).

Цель исследования является повышение производительности приложений, использующих алгоритмы сортировки. Для достижения поставленной цели необходимо решить задачу сравнения указанных методов сортировки для грамотно подобранных условий и данных.

Результатом работы является приложение на языке C#, написанное с использованием технологии Windows Forms, которое позволяет проводить сравнения эффективности различных алгоритмов сортировки для одинаковых заданных условий, с последующим выводом результата сравнения.

Сравнение осуществляется как по времени, так и по количеству действий, требуемых каждому алгоритму для конкретного случая. Такая реализация позволяет выделить наиболее эффективные алгоритмы сортировки для каждой ситуации.

Таким образом, в данной работе было проведено сравнение таких алгоритмов сортировки: пирамидальный, быстрый и пузырьковый. Планируется рассмотреть и другие алгоритмы.

UDC 629.735.7

SYSTEM OF QUADCOPTER

Ouafa Dahibi, Student of group 220F,
National Aerospace University named after
N.E. Zhukovsky "KhAI"

Introduction. A quadcopter is a multirotor craft that is lifted and propelled using four rotors. The propellers of a quadrotor are vertically oriented and each of them works in varying speeds, giving the aerial vehicle some speed, desired thrust and turning force, required in moving the quadcopter on the air. Typically, the quadcopter has the following configurations; two rotors turning clockwise and the other two turning counter clockwise, helping the quadrotor respond to controls of its pilot when flying.

Motivation. Drones and quadcopters have revolutionized flight. They help humans to take to the air in new, profound ways. Today's drones and quadcopters come with mind-blowing capabilities, flight being the least of these. These nifty devices capture dazzling aerial images and enable augmented reality game playing as well.

They can go to places humans cannot, enabling them to do much more than thought possible.

How these devices developed over the decades is fascinating. Their aerodynamic features and uses pique curiosity.

Goal. Drones and quadcopters, with extensive history and capabilities, are the devices of the future. In time to come, humans will find it difficult to imagine life without them, the goal of this research is to give a global idea about the importance and the role of quadcopters to improve our life for better.

Results. Quadcopters are great toys. However, the technological world is dynamic and improvements are being made on this craft, creating more excitement in understanding how they work and their potential benefits.

UDC 004.89:61

INTERNET OF THINGS: HEALTHCARE AND MEDICINE

Labatt M.A., Student of group 555f,
Scientific advisor Vyacheslav Kharchenko,
National Aerospace University named after
N.E. Zhukovsky "KhAI"

Introduction. Nowadays, global ageing and the prevalence of chronic diseases have become a common concern. A promising trend in healthcare is to move routine medical checks and other healthcare services from hospital to the home environment. By doing so, firstly, the patients can get seamless healthcare at anytime in a comfortable home environment; secondly, society's financial burden could be greatly reduced by remote treatment; thirdly, limited hospital resources can be released for people in need of emergency care.

Motivation. Even though the healthcare industry has been slower to adopt Internet of Things technologies than other industries, the Internet of Medical Things (IoMT) is poised to transform how we keep people safe and healthy especially as the demand for solutions to lower healthcare costs increase in the coming years. The IoMT can help monitor, inform and notify not only care-givers, but provide healthcare providers with actual data to identify issues before they become critical or to allow for earlier invention.

Risks and challenges. One of the major risks associated with the erosion of IoMT is the privacy of patient sensitive data. Patient history confidentiality is mandatory in the healthcare sector and critical data may be misused if accessed by miscreants. Intentional disruption and manipulation of networks is another threat faced by IoMT in the healthcare industry. Similar to any networked technology, IoMT is vulnerable to hackers, thieves, and spies etc. who may create havoc through medical crime.

Results. Consumers, patients and those working in medical professions will all need to alter their mindsets to take full advantage of this revolution in healthcare and be provided with innovative methods to motivate a change in behavior. And so, it will be the companies who are able to offer cutting-edge, highly personalized solutions – that are both meaningful and trustworthy – who will become our new health mentors.

УДК 621.311.25: 621.383.4

РАЗРАБОТКА УСТРОЙСТВА ДЛЯ АВТОМАТИЧЕСКОГО ПОЗИЦИОНИРОВАНИЯ ПАНЕЛЕЙ СОЛНЕЧНЫХ БАТАРЕЙ

Сверчков Д.А., студент 525б гр.
Научный руководитель: ст. преподаватель А.Е. Перепелицын
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

В наше время солнечные батареи обретают все большую и большую популярность. Они обширно используются не только в регионах с тропическим и субтропическим климатом, а почти во всех уголках нашей планеты. Обычно солнечные батареи располагаются на крышах домов, однако из-за того, что это их положение статично, ресурс используется неэффективно.

В итоге, целью данной работы является повышения эффективности использования солнечных батарей, которые используются для выработки электроэнергии. Для достижения поставленной цели, необходимо решить задачу разработки программной и аппаратной части некого устройства, которое будет наиболее эффективно позиционировать солнечные батареи по отношению к солнцу.

Проведенный анализ проблемы показал, что важной проблемой является эффективность позиционирования батарей по отношению к солнцу.

Разработанное устройство решает данную проблему, оно позволяет максимально эффективно использовать плоскость солнечной батареи, умно регулируя положение батареи по отношению к солнцу в двух осях.

Данная система работает следующим образом. Производится автоматический поворот панелей в зависимости от положения солнца. Положение солнца определяется на основании данных, полученных с четырех фоторезисторов и расчета разницы в их показаниях. Данное устройство не нуждается в первоначальной настройке и готово к работе сразу после установки.

UDC 629.7.014-519;681.518.3

INVESTIGATION OF THE SHAPE OF AN ULTRASONIC SIGNAL REFLECTED BY AN UNEVEN SURFACE

Parfenova I.V., Student of group 550M,
Scientific advisor: Dr. Popov A.V.,
Language advisor: Senior lecturer Babakova L.M.,
National Aerospace University named after N.E. Zhukovsky "KhAI"

Nowadays, unmanned aerial vehicles (BPLA) are increasingly being used to solve the problems of surveying areas of natural disasters and man-made disasters, monitoring buildings and structures, search and rescue operations, protecting the state border, etc. The current trend in the development of BPLA is their intellectualization. The main requirement for such BPLA is ability to perform a flight mission at any time of day in difficult meteorological conditions in presence of unobtrusive obstacles to flight.

One of the claimed "intelligent" functions of BPLA is the automatic selection of a landing site in the given area, especially when an emergency landing. Particularly challenging this problem is for multiplex type BPLA due to their design features this means landing on an uneven surface may lead to the breakdown of aircraft propellers. It has been noticed that protective covers installed in a number of models significantly deteriorate the aerodynamic.

The most common data is that obtained and used for selecting the landing site from an on-board video camera or a laser altimeter scanner. An alternative is ultrasonic sensors, whose performance, unlike optical systems, does not depend on the level of illumination and the degree of smog in the atmosphere. However, the known models of ultrasonic range finders and altimeters determine only the distance to the nearest obstacle.

This work is devoted to an experimental study that shows that the shape of the reflected ultrasonic pulse depends on the degree of unevenness of the reflecting surface.

The report presents the results of experimental studies of ultrasonic signals reflected by surfaces with varying degrees of unevenness. It is shown that the shape of the reflected signal makes it possible to determine the height of the surface irregularities.

UDC 351.814.3

LIGHTS IN AVIATION – THEIR USES

Dube Mandlaenkosi. B, Student of group 330F,
National Aerospace University named after
N.E. Zhukovsky "KhAI"

Introduction. Lights play a fundamental as well primary role all across the aviation industry for various purposes. We tend to take them for granted when we see them in airports or planes and never put much significance to them not knowing that they are there for a particular reason playing a very vital role. Airport lights come in different shapes, sizes and colors all signifying some very crucial information for the people who work or use the airport such as pilots, engineers and people who offer services in airports. Aircraft lights also tell necessary aspects of the aircraft such as its wing and fuselage size. Internally there are a lot of lighting systems with their own uses and meanings.

Motivation. Passengers now play a bigger role while travelling be it as extra eyes at the airport and during flights and during times of emergency. The more informed the passengers are the easier it is for everyone to help in times of crisis or to even avoid crisis. Due to increasing complexity of today's airport and aircraft lighting systems, special awareness is needed to enlighten not only professionals but everyone in general. When passengers understand and know what they are using and what is around them they tend to feel at ease and enjoy using those things, I want to bring that same feeling to this wonderful industry that I am a part of.

Goal. The goal of my article presentation is of deeper and clearer understanding of the important role lights play in the aviation world.

UDC 550.837.7

AIRBORNE WEATHER RADAR

Ben Hassen Jehan, Student of group 120F,
National Aerospace University named after
N.E. Zhukovsky "KhAI"

Airborne weather radar is a type of radar used to provide an indication to pilots of the intensity of convective weather. Modern weather radars are mostly doppler radars, capable of detecting the motion of rain droplets in addition to intensity of the precipitation.

Typically, the radar antenna is located in the nose of the aircraft. Signals from the antenna are processed by a computer and presented on a screen which may be viewed by the pilots. Droplet size is a good indicator of strong updrafts within cumulonimbus clouds, and associated turbulence, and is indicated on the screen by patterns, color coded for intensity. Some airborne weather radar systems may also be able to predict the presence of wind shear

During World War II, radar operators discovered that weather was causing echoes on their screen, masking potential enemy targets. Techniques were developed to filter them, but scientists began to study the phenomenon. Soon after the war, surplus radars were used to detect precipitation. Since then, weather radar has evolved on its own and is now used by national weather services,

Airborne weather radar is one of the most important tools in airplane, we didn't make a huge improve for it. Regardless that it is one of the factors to protect the airplane, in order for pilots to successfully use weather radar to keep them out of trouble, they need to have a good understanding of how weather radar works, how to use the technology and how to interpret the information and display.

The knowledge it is the secret for improving and developing everything, and airborne weather radar it is one of safety tools in airplane, so it need to be developed continuously this device used to locate precipitation, calculate its motion, and estimate its type (rain, snow, hail etc.). Modern weather radars are mostly pulse-Doppler radars, capable of detecting the motion of rain droplets in addition to the intensity of the precipitation. Both types of data can be analyzed to determine the structure of storms and their potential to cause severe weather.

UDC 004.052

RELIABILITY ASSESSMENT OF INTERNET OF THINGS IN SMART HOME

Salahdine Khiarhoum, Student of group 555f,
Scientific advisor Vyacheslav Kharchenko,
National Aerospace University named after N.E. Zhukovsky "KhAI"

Introduction. With the advent of the Internet at the end of the 21st century and the vast amount of information being exchanged on the Web Our lives are gradually changing and we rely more on the Internet in many things. Internet uses are no longer limited to computers and some traditional devices, but they are beginning to fall within the scope of things we use in our daily lives The rapid proliferation and multiplicity of devices connected to the Internet within the institutions, streets and houses assures us We're moving toward the concept of internet of things at a rapid pace.

Motivation. Laziness and love of relaxation is one of human qualities and the human mind is not infallible from mistakes Since houses are the most places where we must feel safe and everything is fine and make sure the safety of our children in their rooms and make sure the validity of eating inside the refrigerator and control all appliances and energy at home by connecting multiple devices to the Internet and exchange information stored and send results to the user.

Goal. The goal is to assess reliability of IoT in smart home taking into consideration, availability, safety, and security. IoT can only be a better technology if all those attributes are not overseen because they are the core of any successful computer system.

Results. The result of this paper will prove how IoT is a successful technology in connected homes. It will prove how people can control their home and know what takes place in real time because their home will be safely connected. It will reduce the amount of time people spend doing home activities.

UDC 004.052

WORK AUTOMATION IN SALES DEPARTMENT

Tavrin A.V., Student of group 525,
Scientific advisor Anatolii Shostak,
National Aerospace University named after
N.E. Zhukovsky "KhAI"

Today, we can see that programs, algorithms, products of IoT or AI technologies not only can take the big part of non-creative and repeatable work from humans. Today, IT-specialists have the great advantage to implement their skills and knowledge in order to make our world a better place for millions of people – make their work less laborious and sometimes even less dangerous.

The same can be said about development of the program products on the stage of sales process. In order to make the database of interested clients – so called leads, sales managers should make numerous amount of repeatable actions, searching for the right people at target groups or markets. This is called lead generation.

The idea of saving time and money for the Sales Department I am working in has inspired me to start working on my project. My result – database containing the main information about customers and clients of the company.

The brief analysis showed me, that today the sales departments in IT companies use different systems and products to automate and speed up their work. Among them: Salestools and Briteverefy. These program services allow you to perform an effective search in categories such as occupation, country or native language of entrepreneurs, in order to continue to produce email newsletters, saving all data about it in the database. Using my future application, I will be able to make more individually approach the process of working with a large number of user data and more effectively automate the process of sending messages.

The project has prospects for development in many ways that I have already mentioned above, talking about the future of my project. Moreover, a lot can be done in the field of automation of work with professional contacts services of social networks such as LinkedIn or Xing. In the future, I am planning to create and develop additional functionality.

УДК 628.976

ДИНАМИЧЕСКАЯ ФОНОВАЯ ПОДСВЕТКА ЭКРАНА МОНИТОРА НА ARDUINO NANO

Федько А.Д., студент 525-А гр.,
Научный руководитель: ст. преподаватель Перепелицын А.Е.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Фоновая подсветка снижает нагрузку на глаза при работе в темное время суток. Это достигается за счет отсутствия резкого перехода между освещенностью экрана и за экранной поверхностью. Подсветка визуально расширяет картинку и добавляет эффект присутствия при просмотре фильмов и в играх.

Целью данного проекта является повышение комфорта при эксплуатации мониторов в условиях слабой освещённости. Для достижения данной цели необходимо решить задачу разработки экономически обоснованного прототипа фоновой подсветки с большим разрешением.

Проведенный обзор существующих решений показал, что в качестве примера для разработки фоновой подсветки для монитора может выступать технология Philips Ambilight. Такая подсветка будет использоваться на мониторах компьютеров, ноутбуков и экранах телевизоров, подключенных к компьютеру.

В качестве целевой платформы для аппаратной реализации выбрана плата Arduino Nano 3.0. Для реализации подсветки будет использоваться адресная светодиодная лента на чипах WS2812. Для реализации настройки яркости подсветки будет использоваться фоторезистор 5528 LDR. Для захвата изображения с экрана под Windows будет использоваться программа AmbiBox, а в Mac OS X и Linux – программа Prismatik.

Полученное устройство сможет создавать фоновую подсветку монитора. Каждый светодиод будет отображать цвет экрана рядом с ним, что даст эффект выхода изображения «за рамки». С помощью фоторезистора будет регулироваться необходимая яркость подсветки, что также позволит автоматически отключать подсветку, когда она не нужна.

Таким образом, данная подсветка позволяет повысить комфорт при эксплуатации и заменить дорогостоящие аналоги.

UDC 004.7

THREAT MITIGATION FOR OPENSTACK CLOUD: DRIVERS AND STOPPERS

Alanamu M.A., Student of group 555f,
Scientific advisor Dr. S. Martinenko,
National Aerospace University named after N.E. Zhukovsky "KhAI"

This paper focuses mainly DDoS and mitigation techniques in openstack cloud. Academic researchers or students have a great benefit when using the cloud infrastructure for research purposes, researcher can also use trystack account if there's no memory of the systems. A contribution of their Cloud Files platform by Rackspace, combined with the Nebula computing software from NASA led to the initial birth of OpenStack. In the time since its inception, the OpenStack consortium has managed to bring in over 100 members, including high profile industry names such as Citrix, Canonical and Dell.

A DDoS attack targets resources or services in an attempt to render them unavailable by flooding system resources with heavy amounts of unreal traffic. The objective of DDoS attacks is to consume resources, such as memory, CPU processing space, or network bandwidth, in an attempt to make them unreachable to end users by blocking network communication or denying access to services.

Use quotas per domain, project and per user and implement OpenStack high availability best practices. HA architecture assumes redundancy, so you can safely isolate or shutdown the affected instance and the remaining instances should be able to function normally. Use OpenStack availability zones for physical isolation or redundancy. HTTP reverse proxies for REST API endpoints and HTTP applications in the DMZ that can be used to isolate OpenStack services from a direct access. Each reverse proxy can be a Linux server with a minimal set of packages. Such a proxy can be easily maintained and also can be used as HTTP load balancer, HTTP accelerator (for encrypted connections) and security gateway to efficiently mitigate DoS/DDoS attacks.

UDC 523.43

COLONIZATION ON MARS

Bansi Parsania, Student of group 133f,
National Aerospace University named after
N.E. Zhukovsky "KhAI"

Introduction. The economic viability of colonizing Mars is examined. It is shown, that of all bodies in the solar system other than Earth, Mars is unique in that it has the resources required to support a population of sufficient size to create locally a new branch of human civilization. The potential of relatively near-term types of interplanetary transportation systems is examined, and it is shown that with very modest advances on a historical scale, systems can be put in place that will allow individuals and families to emigrate to Mars at their own discretion.

Motivation. The primary "win" of accomplishing human exist-ence as a multi-planetary species would be lowering the risk that humanity could ever be obliterated by one extinction level event in any single location.

Of course, space exploration and colonization would:

– lead to a new path in human evolution;

– be an experience, as a species, that would bring discoveries;

– give humans new perspectives about the galaxy, Mars, and human life.

Goal. The goal of our research is to provide humanity a new infection or disease free home and evolution of new species of human. An evolution and exploration of space will be a biggest achievement human will remember for next 1000 years from now .

Results. To achieve a self-sustaining society you'll need to send 1 million people to Mars which could take 40-100 years. To get those people there Musk introduced the SpaceX Interplanetary Transport System. The rocket, largest ever built, could carry 100 plus people per flight and would need 10,000 flights to carry those million people. According Elon Musk hopes to be able to eventually carry 200 people per flight which would reduce number of flights needed.

UDC 004.351.321

AUTOMATION OF TECHNOLOGICAL PROCESSES IN MANUFACTURING INTERNET OF THINGS CONTEXT FOR PHARMACEUTICAL ENTERPRISES

Demidenko D.V., Student of group PR-424,
Scientific advisor Alina Fedoseeva,
Kharkiv Radiotechnical School "HRTT"

The industrial I&C systems have evolved over the years. Now this kind of systems, such as ERP, MRP, MES, are necessary for use in the critical branches. In the future it is necessary that the software logic of the automatic process control system should be a «cloud of control» and allow to connect with different types of objects: HMI, equipment, technological lines ets. Today we have a new notion – manufacturing internet of things (MIoT), which must be embedded in the technological process of the pharmaceutical enterprises. And the article are considered the questions of applicability of MIoT technologies in the pharmaceutical industry.

Manufacturing Internet of things now is the automation of production processes with networks connections. In the different types of equipment are used in the technological drugs production at the different stages. Each of this type of equipment has a sensors and detectors for monitoring of the progress of the technological process. Optical sensors are used in pharmaceutical manufacturing to measure optical properties within the framework of product quality control and when checking the correctness of marking and packaging of drugs. In this regard, there is a need for technology that allows the management of the production process through network technologies. But immediately the question arises about the safety of the use of such technologies in critical industries and in pharmaceutical production in particular. It is necessary to be able to track the workload of the data transmission channels of the equipment sensors to ensure high-quality and safe technological operation.

Results of this paper open the possibility of revision and further research will be aimed at improving the methodology for determining the load of control points of technological equipment with the help of MIoT agents.

UDC 004.052

DEVELOPMENT OF LANGUAGE LEARNING TOOL

Peñaloza G.S., Student of group 515B,
Scientific advisor Eugene Babeshko,
National Aerospace University named after
N.E. Zhukovsky "KhAI"

Introduction. Learning foreign languages provide a lot of benefits but could be a challenging task due to the amount of hours of study and practice that is needed, because it is complex especially when they do not have much in common.

Modern technologies could help in this learning process by coupling it with the daily activities we do in front of a computer, especially those leisure hours dedicated to social networks, so we could use our own vocabulary to know how to write and pronounce in a foreign language (in this case in Russian).

Motivation. Currently we live in a very competitive world and if we do not want to stay behind, it is necessary to develop new skills, among these learning a new language is very useful. Although there are many online courses, translators, dictionaries, games, among others, these are usually used only when people are studying. Therefore, this tool aims to be in constant practice and learning based on the words that are often used while surfing the Internet.

Goals. The objective of this research is to learn Russian language vocabulary always while we carry out activities on our computer, through the implementation of a language learning tool.

Results. After research was performed, a tool was developed that helps the user to learn their own vocabulary in the Russian language while using their computer. This software captures the words that use the most on a day-to-day basis and present them in a visual and audio way every time you use it again. This vocabulary that is created from the user (or entered by opening the software) will be stored, translated (using Google Translate) and classified as well as allowing to verify what has been learned.

This tool is intended to add the possibility of choosing other languages, a better interface and presentation of advanced statistical data and multiplatform since currently the use of smartphones is greater. (51.2% in 2016 according to StatCounter).

УДК 004.75

РАЗРАБОТКА СРЕДСТВА КОНТРОЛЯ ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ РАБОЧЕГО ВРЕМЕНИ

Поповиченко О.Н., студентка 525 гр.,
Научный руководитель: ст. преподаватель, Перепелицын А.Е.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

На сегодняшний день, одной их самых распространённых причин отклонения от намеченного срока выполнения проектов в IT компаниях является нерациональное распределение времени сотрудниками, что в свою очередь, приводит к неэффективной работе, задержкам, неправильным выводам при анализе этих задержек и, как следствие, несвоевременному выходу продукта на рынок, когда в нём уже нет необходимости.

Также существуют люди, которые работают сами на себя. Как правило, доход фрилансера зависит от времени, потраченного на разработку продукта. Поэтому для таких людей, а также заказчиков программных продуктов, время – это деньги.

Целью данной работы является повышение эффективности использования рабочего времени. Для достижения поставленной цели необходимо решить задачу разработки сервиса, предназначенного для координации и планирования рабочего времени для эффективного его использования.

Аналитический обзор существующих решений показывает, что общей их чертой является планирование времени с учетом расписания отдельного человека для каждого дня недели, а большинство из них позволяет формировать отчет со статистикой временных затрат на выполнение конкретной задачи.

Разрабатываемая система представляет собой web-сервис. Обращение к сервису происходит посредством браузера. Сервис позволяет отслеживать время, потраченное на выполнение той или иной задачи, привязывать задачи к проектам, создавать отчет по проектам.

Основными используемыми технологиями в составе разрабатываемого сервиса являются: JavaScript, MySql и NodeJS.

В дальнейшем планируется развертывание сервиса для тестирования на пробной группе пользователей.

УДК 004.421

АНАЛИЗ АЛГОРИТМОВ ЭВРИСТИЧЕСКОГО ПОИСКА

Титаренко В.С., студентка 525 гр.,
Научный руководитель: к.т.н., доцент Шостак А.В.
Национальный аэрокосмический университет
им. Н.Е. Жуковского «ХАИ»

Искусственный интеллект (ИИ) – свойство интеллектуальных систем выполнять творческие функции, которые традиционно считаются прерогативой человека.

Задача поиска кратчайшего пути может быть решена с использованием алгоритма ИИ.

Для того чтобы эффективно выбирать одну или несколько лучших гипотез, избегая комбинаторного взрыва, используются алгоритмы поиска в пространстве состояний.

Если задаться целью обойти пространство состояний, то потребуется экспоненциальное время. Чтобы избежать этой проблемы, принимаются следующие типы алгоритмов: полный перебор и эвристический поиск.

Эвристический поиск основан на функции оценки состояния, что позволяет ранжировать пространственные состояний и ищет в пространстве состояний более целенаправленно, чем алгоритмы полного перебора.

Целью данного исследования является повышение производительности приложений, использующих алгоритмы поиска. Для достижения поставленной цели необходимо решить задачу анализа существующих алгоритмов эвристического поиска.

Для сравнения были выбраны алгоритм лучевого поиска, A* и алгоритм Дейкстры, так как первый является одной из попыток улучшения поведения жадного поиска, исправить присущие ему проблемы - конечные состояния зачастую достигаются слишком длинным, неоптимальным путем.

Основной минус лучевого поиска в том, что, в отличие от жадного, лучевой поиск не гарантирует нахождения конечного состояния с наилучшим качеством. Плюсом же является то, что можно настраивать ширину фронта. Чем фронт уже, тем быстрее работает алгоритм, но тем чаще он ошибается. Чем шире фронт, тем алгоритм работает лучше, но дольше.

УДК 004.032

АКТУАЛЬНОСТЬ И ПРОБЛЕМАТИКА ПРАКТИЧЕСКОГО ИСПОЛЬЗОВАНИЯ ЦИФРОВОГО ЗВУКА И DAW

Лаврик И.С., ученик 10-А класса,
Научный руководитель: ассистент кафедры 503 Егорова Е.В.
Аэрокосмический лицей на базе НАУ «ХАИ»

В прошлых веках – музыка была вещью элитарной и доступной только до весьма успешных людей, чьи семьи могли себе позволить обеспечение своих детей инструментом и образованием. Кто-то становился великим композитором, кто-то простым бардом. В наше время, музыка стала общедоступной затеей, ибо перестала нуждаться в физическом носителе как инструмент. С появлением цифрового звука и таких вещей как музыкальные секвенсоры или же DAW (Digital Audio Workstation) – музыка стала доступна для всех слоев общества. Однако кроме эстетического применения, тип данного программного обеспечения имеет и практическое значение. О чем собственно и пойдет дальше речь.

Целью данной работы является анализ и расширение спектра практического применения цифрового звука и DAW. Для достижения этой цели необходимо рассмотреть проблемы цифрового звука и DAW и их предположительное решение.

В данный момент существует множество музыкальных технологий и программного обеспечения, что значительно улучшило и развило возможности звука. В наше время самые популярные DAW это FL Studio, Cubase, Nuendo, Reaper, Ableton. Все эти программы имеют свои плюсы и минусы и каждая из них используется в разных аспектах sound produce-инга.

Проведенный анализ показал, что у звука и конкретно DAW есть множество применений в других сферах кроме эстетической, такой как реклама и мультимедиа.

Таким образом, sound и DAW имеет большие перспективы для развития. Музыкальные технологии, такие как микрофон и граммофон, которые изменили историю XIX – XX веков, имеют большое будущие и будут внедряться в жизнь человека все больше и больше, ибо звук – является одним из самых сильных способов контроля и передачи информации.

УДК 004.021

ЗАДАЧА О РЮКЗАКЕ

Герус В.А., студентка 515 гр.
Научный руководитель: старший преподаватель Дужая В.В.,
Национальный аэрокосмический университет
им. Н. Е. Жуковского «ХАИ»

Как в давние времена, так и сегодня люди стараются использовать оптимальные пути решения поставленных задач: как избежать убытков, создать максимальное количество безопасных дорог и найти самый короткий путь. Данные вопросы рассматриваются в комбинаторной оптимизации. Одной из таких задач является задача о рюкзаке.

Целью данной работы является написание программы, которая решает следующую задачу: имеется некоторое количество предметов, известны вес каждого предмета и его стоимость. Определить, какие предметы нужно положить в рюкзак, чтобы общий вес не выходил за данную границу, а общая стоимость была максимальна. Вес рюкзака не должен превышать 50кг.

Программа запускается в консольном режиме. Все данные вводятся с клавиатуры: количество предметов, вес и цена каждого предмета. Решение производится за счет вывода игроком номера предмета, который необходимо положить в рюкзак. Чтобы программа работала корректно, используется проверка вводимых данных. Для этого были использованы операторы условия и цикла. После выполнения условия пользователем программа выводит свой вариант, чтобы игрок проверил правильность выполнения задачи.

Программа написана на языке C, среда разработки – Microsoft Visual Studio.

УДК 004

ПРОГРАМНА РЕАЛІЗАЦІЯ АЛГОРИТМУ РОЗПІЗНАВАННЯ ФІЗИЧНИХ СХЕМ ТА ПОКАЗНИКІВ ФІЗИЧНИХ АНАЛОГОВИХ ПРИБОРІВ У РЕАЛЬНОМУ ЧАСІ «RECOON»

Казаков Г.С., Тимошевський Д.С., учні 11-В класу,
Научный руководитель: учитель інформатики Єфімова Я.В.,
Комунальний заклад «Обласна спеціалізована школа-інтернат II-III ступенів «Обдарованість» Харківської обласної ради»

У сучасному світі панівне місце зайняли розвиток програмної інженерії та технологічний прогрес. Можливості комп'ютера вже не мають меж, з його допомогою можна навіть розпізнавати об'єкти. Така можливість є дуже корисною, адже програми з розпізнавання можна використовувати у системах пошуку і охорони, наукових дослідженнях та експериментах.

Актуальність роботи пов'язана з постійним розвитком та удосконаленням технологій розпізнавання образів, відсутністю реальних рішень у розпізнаванні схематичного подання схем.

Предметом дослідження є алгоритми та способи розпізнавання образів з використанням бібліотеки OpenCV.

Об'єктом дослідження є процес розробки тестування та представлення власної програмної реалізації з теми роботи. Кінцевим результатом є програма «RECoon» для розпізнавання електричних схем та фізичних аналогових приборів.

Метою роботи є дослідження шляхів та способів реалізації розпізнавання схем та визначених об'єктів у реальному часі; розробка кінцевого програмного продукту, який буде орієнтований під розпізнавання фізичних схем, їх елементів (амперметр, вольтметр, конденсатор, батарея, резистор, лампа), та показників фізичних аналогових приборів у реальному часі.

Завдання роботи, за допомогою яких була втілена мета:

– вибір програмних засобів та технологій, які зосереджені на розпізнаванні образів;

– аналіз засобів реалізації розпізнавання зображень з використанням бібліотеки OpenCV;

– реалізація власного проекту, який відповідає заявленій темі, має прикладне значення та може використаний у різних напрямках дослідження.

УДК 004.056.55

РАЗРАБОТКА ПРОГРАММЫ ДЛЯ ИЗУЧЕНИЯ ОСНОВ КРИПТОГРАФИИ C.G.LEARN

Лаптев А.А., ученик 9 класса,
Научный руководитель: учитель информатики Ефимова Я.В.
КЗ ОСШИ «Одарённость»

Защита цифровой информации в современном мире - одна из самых актуальных тем нашего времени, ведь большинство организаций хранят в цифровом виде именно важную информацию. Поэтому активно развивается такая наука как криптография. Безусловно современные схемы Bob, Alisa, Eva являются доступными для большинства пользователей, однако в большинстве статей посвященных этой теме собрано большое количество терминов непонятных рядовому пользователю.

Целью данной работы является разработка программы, в которой довольно открыто и доступно, графическим методом, будет объясняться тот или иной алгоритм шифрования. Так же будут видео уроки, предназначенные для пользователей, уже ознакомленных с основами криптографии, однако все также не понимающих принципы ее действия.

На данный момент выделяются несколько проектов, среди которых самая известная программа Cryptoy выпущенная британской спецслужбой GCHQ.

Для выполнения цели данной работы были определенны следующие задачи:

– изучить различные алгоритмы шифрования данных;
– составить список алгоритмов, которое будут задействованы в программе;
– практически реализовать собственное ПО - C.G.Learn;
– сконцентрироваться на улучшении ПО - C.G.Learn.

Языком программирования для достижения данных целей выбран C++ с использованием среды разработки Microsoft Visual Studio.

УДК 004.9.615.12

ОСОБЕННОСТИ РАЗРАБОТКИ РПГ-ИГР В СРЕДЕ РАЗРАБОТКИ RPG MAKER

Лаптий А.А., студент ПР-424 гр.,
Научный руководитель: преподаватель Федосеева А.А.
Харьковский радиотехнический техникум

На сегодняшний день гейм-индустрия занимает одно из первых мест в жизни многих людей. Специфика индустрии компьютерных игр очень близка к другими отраслями развлечений (например, киноиндустрия).

Game-индустрия зачастую характеризуется: малой прибылью для создателей, впрочем, это благоприятствует большому количеству независимых разработок; наличием сложноформализуемого понятия «Fun»; поддержкой основных платформ: Windows (EXE), Mac OS X (APP), Android (АПК), iOS (IPA) или HTML5 для веб-браузеров. Благодаря всему этому, повышен спрос на разработчиков и проектировщиков аутентичных игровых приложений.

В рамках данной работы рассматривается процесс разработки РПГ игры «Unicorn Adventures» с использованием среды RPG Maker. Эта игра представляет собой РПГ-игру, в которой различные персонажи могут передвигаться по карте, находить различные предметы и

В рамках разработанного приложения с помощью текстур для конкретных карт, создан дизайн базовых локаций, подземелий, боевых полей. К тому же, сама среда предоставляет большой выбор стандартных карт.

Все персонажи, их умения, боевая система, возможность анимации добавлены с помощью базы данных, заполняемой в рамках RPG Maker. Данная БД представляет собой доступный, интуитивно понятный набор инструментов для обеспечения высокой степени контроля над будущей игрой. Карта позволяет осуществлять управление действиями персонажа, можно выбирать умения для конкретного персонажа в рамках игры.

Таким образом, было создано игровое ПО, прошедшее полный цикл разработки, представляющее собой РПГ с дружелюбным интерфейсом и полным набором функционала.

УДК 004.021

ИГРОВАЯ ЗАДАЧА «ЦЗЯНЬШИДЗЫ»

Белоус Н.К., студент 515и гр.,
Научный руководитель: ст. преподаватель Дужая В.В.
Национальный аэрокосмический университет
им. Н.Е.Жуковского «ХАИ»

Игровая индустрия – одна из самых интенсивно развивающихся сфер развлечений. Хотя игр написано великое множество, они продолжают выпускаться каждый год, причем их разрабатывают и огромные игровые корпорации, и отдельные программисты, большие проекты и маленькие задачи.

Многие программисты начинают пробовать свои силы в разработке игр с самого начала обучения. Часто даже маленькие задачи могут принести большой опыт из-за сложной реализации.

Цель работы – написание китайской национальной игры «Цзяньшидзы». Буквальный перевод названия – “выбирание камней”. Имеется две группы камней и два игрока, которые по очереди берут не нулевое количество камней из одной кучки, или из обеих. Побеждает тот, кто заберёт последний камень из обеих куч.

Программа разработана в консольном режиме с использованием текстового интерфейса. Программа состоит из следующих функций:

rand() – генерация случайных чисел: количество камней в кучках и номер первого играющего;

forder() – вывод количества камней в кучках и номер текущего игрока;

fwinner() – вывод номера игрока, который победил, если камней не осталось.

Среда разработки – Visual Studio 2017, язык программирования – C.

УДК 004.021

ИГРОВАЯ ЗАДАЧА «ХАНОЙСКАЯ БАШНЯ»

Сидоренко Ю.А., студентка 515 гр.,
Научный руководитель: ст. преподаватель Дужая В.В.
Национальный аэрокосмический университет
им. Н.Е.Жуковского «ХАИ»

Игры с давних времен были неотъемлемой частью человеческой жизни. Ведь благодаря играм человек может расслабиться и отдохнуть от повседневной жизни. Или же наоборот, играть в развивающие игры, способствующие логическому мышлению, что очень важно для человека. А может быть так, что игра будет одновременно развивать эрудицию и даст возможность отдохнуть.

Именно поэтому целью данной работы является реализация консольной игры «Ханойская башня».

На доске есть три колышка. На один из них нанизано n дисков, убывающего вверх диаметра. Для победы нужно перенести все диски в том же порядке на другой колышек. За ход можно брать только один диск. Класть больший диск на меньший не разрешается. Количество дисков вводит пользователь, тем самым выбирая сложность этой игры.

Для осуществления данной задачи были реализованы: ввод пользователем номера диска, который нужно перенести и номер колышка, на который нужно положить диск, а также проверки на допустимые действия и корректные данные. Если пользователь вводит некорректные данные или же выполнены условия победы, то выводится соответствующее сообщение. Управление полностью производится за счет клавиатуры. И хотя для данной игры желательно делать графический интерфейс, в данном проекте используется текстовый. Графический интерфейс – это дальнейшее развитие данной работы.

Программа написана на языке программирования Си.

УДК 004

ВЛАСНА ПРОГРАМНА РЕАЛІЗАЦІЯ АЛГОРИТМУ АСИМЕТРИЧНОГО ШИФРУВАННЯ NTRU

Таланцев М.Є., учень 10 класу
Научный руководитель: учитель інформатики Єфімова Я.В.,
Комунальний заклад «Обласна спеціалізована школа-інтернат II-III ступенів «Обдарованість» Харківської обласної ради»

Криптографія як наука не втрачає своєї популярності, а можливі напрямки для дослідження розвиваються та розширюються з кожним днем. Необхідність захисту інформації походить із давніх часів, але вимоги до захисту змінюються, й завжди потрібні нові дослідження щодо оптимізації старих алгоритмів та знаходження нових. У світі існують симетричні та асиметричні алгоритми шифрування. Для дослідження та реалізації ми обрали саме асиметричні через їх більшу криптостійкість.

Отже, робота є актуальною, оскільки асиметричні алгоритми є більш криптостійкими та менш дослідженими, ніж симетричні. У науково-дослідній роботі поставлена задача поширювати популярність асиметричного шифрування на основі аналізу одних із найпопулярніших на сьогоднішній день алгоритмів RSA та менш дослідженого, але більш криптостійкого NTRU. Завданням роботи в результаті порівняння є вибір одного з алгоритмів для власної програмної реалізації, як для функції шифрування інформації, так і для дешифрування.

Предметом дослідження виступають алгоритми асиметричного шифрування RSA та NTRU. Об’єктом дослідження в роботі є процес розробки додатку для шифрування та розшифрування інформації мовою програмування C#.

Метою роботи є деталізоване дослідження алгоритмів асиметричного шифрування RSA та NTRU, розробка криптографічно стійкої системи захисту інформації у вигляді додатку.

Практичне значення роботи полягає в дослідженні найперспективнішого алгоритму асиметричного шифрування NTRU для подальшого розвитку та використання в усіх напрямах захисту інформації. Важливою складовою практичної частини є власна програмна реалізація цього алгоритму в вигляді проекту SHIELD.

УДК 519.686

ОРГАНІЗАЦІЯ АРИФМЕТИКО-ЛОГІЧНОГО ПРИСТРОЮ КОМП'ЮТЕРА

Кузін А. В., студент ОТ-335 гр.
Науковий керівник: Бездітко О.М.
Харківський радіотехнічний технікум

Операційна частина потужних сучасних комп'ютерів являє собою дуже складний пристрій числової програмної обробки дискретної інформації. Для будови блоків операційного пристрою використовуються типові операційні елементи: регістри, суматори, дешифратори. Компоненти, з яких побудовані логічні елементи, мають велику щільність їх упаковки в об'ємі кристалу фізичного матеріалу мікропроцесора.

Обладнання АЛП комбінаційного типу та його регістрове оточення складають по суті обчислювач. Вхідні регістри тимчасового збереження даних забезпечують роботу арифметико логічного пристрою, у якому формується програмно передбачено необхідний результат. Регістри RGX, RGY є приймачами першого та другого операндів відповідно. Регістр RGZ є буфером пам'яті другого операнду з метою після сформованого результату в АЛП завантаження його в регістр RGX. Операційний пристрій регістрового типу, на відміну від акумуляторного, не передбачає завантаження результату на місце тимчасового збереження першого операнду в RGX. Результат зберігається в приймачеві, який передбачається командою. Збереження в регістрі RGX приховане та необхідне для формування частки прапорів стану.

Логічна схема АЛП комп'ютера має гіпотетичний характер наближений до реального. В схемі відсутні зв'язки між регістрами та комбінаційною частиною при виконанні команд множення та ділення, реалізації функціональних зсувів даних.

Комбінаційна частина АЛП доповнена вхідними регістрами для тимчасового збереження операндів і допоміжної комбінаційної логіки формування вхідного та обчислення вихідного перенесень. Програмного доступу до регістрів оточення комбінаційної частини АЛП, виключаючи регістровий файл та регістр прапорів, не має.

УДК 004.021

ОБУЧЕНИЕ ПЕРЕВОДУ В РАЗЛИЧНЫЕ СИСТЕМЫ СЧИСЛЕНИЯ

Кирьян Е. П., студентка 515и гр.
Научный руководитель: ст. преподаватель Дужая В. В.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Система счисления – символический метод записи чисел, представление чисел с помощью письменных знаков. В повседневной жизни мы используем десятичную систему счисления. Однако эта система не всегда удобна. Например, в вычислительной технике применяется двоичная и шестнадцатеричная системы счисления. Поэтому перевод из одной системы счисления в другую часто используется именно там.

Целью данной работы является обучение переводу из одной системы счисления в другую.

В программе существует 3 режима:

– Теория. В этом режиме пользователю в доступной форме объясняется как переводятся числа из одной системы счисления в другую. Предусмотрены системы счисления от двоичной до тридцатипятиричной.

– Обучение. В этом режиме пользователь обучается переводу из одной системы счисления в другую. Для этого пользователь вводит систему счисления, само число и систему счисления, в которую нужно перевести. Предусмотрена проверка на некорректно введенные данные.

– Калькулятор. В этом режиме можно узнать результат перевода из одной системы счисления в другую.

Программа реализована на языке С в среде Visual Studio.

УДК 004.021

ОБУЧЕНИЕ ПЕРЕВОДУ В РАСПРОСТРАНЕННЫЕ СИСТЕМЫ СЧИСЛЕНИЯ

Хмелевцова М.А., студентка 515а гр.
Научный руководитель: ст. преподаватель Дужая В. В.
Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ"

В наше время практически каждый современный человек хоть раз слышал о системах счисления. И каждый знает хотя бы одну из них, десятичную. Десятичная система счисления названа именно так, поскольку в ней 10 цифр, от 0 до 9. Этой системой счисления мы пользуемся каждый день. Но существуют и другие системы счисления. Двоичная и шестнадцатиричная системы счисления используются компьютерами для обработки и хранения информации, а шестидесятеричная система используется для измерения углов и координат – долготы и широты.

Целью данной работы является написание программы обучения переводу чисел из одной системы счисления в другую: из двоичной – в десятичную и обратно, из двоичной – в шестнадцатеричную, из двоичной в восьмеричную и обратно.

На данный момент существует огромное количество различных калькуляторов по переводу чисел из одной системы счисления в другую, их можно найти в браузерах, а также много приложений в Play Market,Appstore и Windows Phone Store. Это говорит о том, что эта тема является очень актуальной на данный момент.

Программа написана с помощью функций. За каждый перевод отвечает соответствующая функция:

– two_ten(),
– ten_two(),
– two_six(),
– six_two(),
– two_eight(),
– eight_two().

Программа реализована на языке С в среде Visual Studio.

УДК 004.3

ПРОГРАМНИЙ КОДЕР/ДЕКОДЕР ПАКЕТІВ ІНФОРМАЦІЇ З CRC15 ЗАХИСТУ ТЕКСТОВИХ ФАЙЛІВ

Гладкова А.О., студентка гр. ОТ-315
Науковий керівник: викладач комп'ютерних дисциплін, спеціаліст вищої категорії Пуйденко В.О.
Харківський радіотехнічний технікум

В теперішній час в комп'ютерних мережах такий аспект, як достовірність інформації є невід'ємним атрибутом протоколів обміну стеку TCP/IP. Відомо, що структура поля «Тип сервісу» заголовку IP - пакету містить поля: D - затримки, T – перепускної здатності та R – надійності, кожен з яких може бути вказаний мережевою операційною системою, як найбільш важливий для передавального вузла комп'ютерної мережі. Як правило, поліпшення одного з параметрів пов'язане з погіршенням інших. Тобто що менше затримка, то вище перепускна здатність каналу, але й зменшується надійність (достовірність, цілісність інформації).

Основною метою представленої роботи є створення програмного кодера/декодера пакетів інформації з CRC15 текстового файлу. При конструюванні програмного коду на мові C++ був використаний систематичний блоковий надлишковий код Боуза – Чоудхурі – Хоквінгема (БЧХ) 31,16 з коректованою здатністю виявлення та виправлення помилок t<=3. Системна програма - кодер перекодовує на боці передавача текстовий файл у відповідності з структурою коду БЧХ 31,16. Бік приймача, при одержанні інформації, активує системну програму – декодер, яка, за необхідністю, виявить та виправить виниклі помилки та представить файл у текстовому форматі.

Таким чином, системний програмний продукт забезпечує додатковий захист інформації, незалежно від значень бітів поля «Типу сервісу» протоколу TCP/IP, що значно підвищує достовірність даних та звільняє мережевий вузол від можливих додаткових запитів на передачу.

УДК 004.032.6

РАЗРАБОТКА ПРИЛОЖЕНИЯ ДЛЯ АВТОМАТИЗАЦИИ И ИССЛЕДОВАНИЯ МЕТОДОВ ИЗМЕРЕНИЯ ВИБРАЦИЙ ПЕЧАТНЫХ УЗЛОВ РАДЕОЭЛЕКТРОННОЙ АППРАТУРЫ

Зиноватный М.А., студент 565М гр.,
Научный руководитель: к.т.н., доцент Куланов В.А.
Национальный аэрокосмический университет им. Н.Е.Жуковского «ХАИ»

Одним из факторов, влияющие на надежность аппаратуры, является вибрация. Специализированные стенды вибродиагностики имеют высокую стоимость.Таким образом, актуальной является задача в использовании, бюджетного варианта, учебного вибростенда для практического исследования проектируемых печатных узлов электронной аппаратуры и создании специального приложения для автоматизации процесса измерений.

В ходе исследований изучено несколько возможных принципов измерения вибраций. Это импульсный и дискретный.

Импульсный метод требует дополнительных исследований, но он является более точным. При воздействии импульса на объект исследования его затухающие колебание будет на частоте собственного резонанса.

Наиболее простом методом измерения амплитудно-частотной характеристики – является дискретное измерение амплитуды вибраций объекта исследования на заданной частоте с последующим объединением полученных данных в единое графическое изображение, которое позволит произвести визуализация результатов амплитудно-частотной характеристики объекта исследований. Выявление частоты резонанса конструкции осуществляется по поиску максимальной амплитуды вибрации на определенной частоте, которая и будет являться частотой резонанса и преобразовываться в специальный сигнал передаваемый через микрофон в разработанное приложение.

Проведенные экспериментальные исследования подтвердили работоспособность данной системы и возможность использования её в учебном процессе.

УДК 004.032.6

АНИМАЦИЯ В WPF

Шевяк К.И., студент 515ст2 гр.,
Научный руководитель: к.т.н., доцент Шостак А.В.
Национальный аэрокосмический университет
им. Н.Е. Жуковского «ХАИ»

По сути, анимация WPF – это просто способ модифицировать значение свойства зависимости через интервалы времени. Поддержка анимации в WPF позволяет применять к элементам управления такие эффекты, как увеличение, дрожание, вращение, создавать интересные эффекты смены страниц и другие.

Например, чтобы заставить кнопку растягиваться и сжиматься, в анимации можно модифицировать ее свойство Width. Чтобы заставить ее мерцать, можно изменять свойства кисти LinearGradientBrush, используемой для ее фона.

За анимацию в WPF отвечает пространство имен System.Windows.Media.Animation. Все классы анимаций можно разделить условно на три группы:

– классы, которые производят линейную интерполяцию значений, благодаря чему при анимации свойство плавно изменяет свое значение.

– классы, которые производят анимацию по ключевым кадрам или фреймам (покадровая анимация).

– классы, которые используют для анимации объект PathGeometry.

Анимацию можно создать и использовать как декларативно в коде XAML, так и программно в коде C#.

Анимация в WPF используется повсеместно и ее разнообразие только повышается.

Ключевыми ролями анимации являеться:

– придание приложению динамичности;

– более удобный и привлекательный интерфейс;

– привлечения внимания, создавая полезные визуальные сигналы.

Анимации имеют решающее значение в WPF из-за динамизма, который они добавляют к пользовательскому интерфейсу. Существует много типов анимаций, в том числе 3D.

УДК 004.032.6

ИССЛЕДОВАНИЕ КЛЕТОЧНЫХ АВТОМАТОВ НА ПРИМЕРЕ ИГРЫ "ЖИЗНЬ"

Третьякова Ю.Ю., студентка 515ст2 гр.,
Научный руководитель: к.т.н., доцент Шостак А.В.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Метод моделирования с помощью клеточных автоматов известен большинству под названием игры "Жизнь". С точки зрения моделирования метод достаточно универсален, он позволяет освоить и прочувствовать элементарные механизмы реализации тех или иных физических или физико - химических законов.

Целью данной работы является демонстрация работы клеточных автоматов на примере игры "Жизнь". В которой моделируется поведение элементов согласно правилам заданным в алгоритме.

Алгоритм «смены поколения» последовательно просматривает все ячейки решётки, определяя судьбу каждой клетки.

Более сложный алгоритм составляет списки клеток для просмотра в последующем поколении.

Конечный автомат представляет собой двумерный массив с двумя входами: предыдущее состояние, получаемое от детектора сигнала, и считанный символ от одного из стеков – для выбора ряда и колонки ячейки.

Игра состоит всего из нескольких простых правил:

– в пустой клетке, рядом с которой ровно три живые клетки, зарождается жизнь;

– если у живой клетки есть две или три живые соседки, то эта клетка продолжает жить; в противном случае, если соседей меньше двух или больше трёх, клетка умирает.

Она более сорока лет привлекает внимание учёных. Игра «Жизнь» и её модификации повлияли на многие разделы таких точных наук, как математика, информатика, физика.

УДК 004.048

ОЦЕНКА ЭФФЕКТИВНОСТИ РАБОТЫ КАПСУЛЬНОЙ АРХИТЕКТУРЫ НЕЙРОННЫХ СЕТЕЙ В СРАВНЕНИИ СО СВЕРТОЧНОЙ АРХИТЕКТУРОЙ

Нгуен А. В., студентка 555М гр.,
Сидоров Я. Е., студент 555М гр.,
Научный руководитель: Кучук Г.А.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Задача обработки и классификации изображения является одной из самых широких областей применения машинного обучения. С увеличением производительности компьютерных систем увеличилась и эффективность обучения алгоритмов, дойдя до той стадии, когда системам на основе нейронных сетей можно доверить выполнение сложных задач, рассчитывая на малый коэффициент ошибки.

Целью данного исследование является изучение и сравнение принципов работы и преимуществ архитектур нейронных сетей для обработки изображений. Для достижения поставленной цели требуется провести анализ коэффициентов эффективности существующих реализаций на основе приведенных алгоритмов.

На данный момент существует две наиболее широко распространенных архитектуры: «Сверточная», предложенная Яном Лекуном в 1988 году, а также «Капсульная», опубликованная Джеффри Хинтоном в 2017.

По итогам проведенного анализа было выявлено, что для обучения капсульной нейронной сети требуется намного меньшая выборка данных, нежели для сверточной. Также новая архитектура демонстрирует оптимальный подход к анализу изображений, учитывая взаимосвязь элементов между собой.

Таким образом капсульная нейронная сеть представляет собой более эффективную альтернативу сверточной архитекруты, что объясняет ее широкое внедрение в решения задач данной области.

УДК 004.043

РАЗРАБОТКА КЛАССА АВЛ-ДЕРЕВА

Андриенко А.И., студент 525 гр.
Научный руководитель: к.т.н., доцент Шостак А.В.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Большинство современных информационных систем содержат в себе базы данных, и к поиску данных в таких базах предъявляются особые требования, такие как максимальная скорость, прогнозируемость времени поиска и точность нахождения информации. Простые алгоритмы перебора не способны обеспечить максимальную скорость и предоставить оценку времени выполнения операции поиска ввиду чего повсеместно заменяются на алгоритмы поиска с использованием двоичных деревьев. Модифицированный вариант двоичных деревьев поиска – АВЛ-деревья, позволяют давать точную оценку скорости выполнения операции поиска данных, а также уменьшает время нахождения искомой информации.

Целью данной работы является увеличение скорости поиска данных в информационных системах путем использования АВЛ-деревьев. Сравнительный анализ быстродействия операций АВЛ-дерева и стандартного двоичного дерева поиска, реализованных на указателях и массиве. Для достижения поставленной цели необходимо проанализировать существующие решения, а также решить задачу разработки класса АВЛ-дерева.

На данный момент существует много вариаций реализации класса АВЛ-дерева, однако все они используют стандартный класс бинарного дерева поиска и повороты вокруг узлов дерева.

Проведенный анализ показывает, что АВЛ-деревья являются наиболее эффективными в обработке ввиду того, что максимальное количество шагов, для обнаружения искомого узла равно высоте дерева, которая является минимальной среди всех существующих двоичных деревьев поиска и максимально приближена к высоте идеально сбалансированного дерева.

Таким образом, АВЛ-дерево - сильная структура хранения, обеспечивающая быстрый доступ к данным.

УДК: 004.622

РЕАЛИЗАЦИЯ ОПЕРАЦИЙ С БИНАРНЫМИ ДЕРЕВЬЯМИ И ОЦЕНКА ИХ БЫСТРОДЕЙСТВИЯ

Тимохин И.С., студент 525 б гр.
Научный руководитель: к.т.н., доцент Шостак А.В.,
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Для решения любой задачи следует выбирать соотвоетсвующую базу, в которую входят определённые структуры данных, среди которых деревья. Для понимания в каких ситуациях рационально применять определённый инструмент, необходимо знать в каких случаях какие деревья наиболее подходящие. В частности бинарные деревья имеют преимущества при поиске, вставке элементов и балансировке. Также применяются в некоторых методах сортировки и криптографических задачах.

Целью данной работы является реализация структуры данных бинарное дерево, анализ сфер его применения, сравнительная оценка операций над деревом, а также анализ преимуществ и недостатков деревьев двоичного поиска. Сравнения с другими видами деревьев. Преимущества и недостатки деревьев двоичного поиска.

Реализация данного исследования деревьев в классическом варианте на C/C++, где есть возможность использовать ссылки на соседние узлы дерева, и, на языках, где применение указателей как таковых запрещено или отсутствует, например в C# ,java и тд. Реализация данного проекта построена на языке C# для раскрытия возможностей ООП в подобных задачах.

Проведённые исследования показывают достоинства и недостатки бинарных деревьев по отношению к другим структурам данных.

УДК 004.021

СРАВНЕНИЕ АЛГОРИТМОВ СОРТИРОВКИ

Кошель М.А., студентка 515 и гр.
Научный руководитель: ст. преподаватель Дужая В.В.
Национальный аэрокосмический университет
им. Н.Е. Жуковского «ХАИ»

Сортировка – последовательное расположение или разбиение на группы чего-либо в зависимости от выбранного критерия. Алгоритм сортировки – это алгоритм для упорядочивания элементов в списке.

Существует большое количество алгоритмов и методов сортировки, которые классифицируют на группы и подгруппы (устойчивые, неустойчивые, непрактичные сортировки и алгоритмы, основанные на сравнениях), имеют свои достоинства и недостатки в разных поставленных задачах (время выполнения, громоздкость процедуры выполнения, количество требуемой памяти для хранения и т.д.).

Цель данной работы состоит в том, чтобы сравнить несколько методов сортировки (пузырьковая, быстрая, вставками, выбором, слиянием) по времени выполнения.

Разработана программа, с помощью которой пользователь может отсортировать одномерный массив, введённый как пользователем, так и с помощью функции rand() одним из предложенных методов сортировки. Программа состоит из следующих функций:

pusir() - функция реализует алгоритм пузырьковой сортировки,
viborom() - функция реализует алгоритм сортировки выбором,
ctrv() - функция реализует алгоритм сортировки вставками,
sliyanie() - функция реализует алгоритм сортировки слиянием,
qs() - функция реализует алгоритм быстрой сортировки.

Построен график зависимостей времен выполнения рассмотренных алгоритмов сортировки в Excel на примерах одинакового ввода массивов.

Программа написана на языке С, среда разработки - Microsoft Visual Studio.

УДК 004.056

СРАВНЕНИЕ СИММЕТРИЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ

Лукьяненко К.С., студент 525-Б гр.
Научный руководитель: к.т.н., доцент Шостак А.В.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

В наше время, как никогда, криптозащита информации является актуальной проблемой. Многие компании вкладывают огромные деньги в развитие и создание новых алгоритмов шифрования данных. Такие алгоритмы должны быть не только надежными, но и эффективными, чтобы быстро справляться с поставленными задачами.

Целью данной работы является исследование существующих симметричных алгоритмов шифрования. Для достижения поставленной цели необходимо разработать программу, реализующую такие алгоритмы шифрования, оценить их надежность и скорость работы с разным набором данных.

Существует большое множество различных алгоритмов шифрования данных, которые, в свою очередь, делятся на симметричные и асимметричные алгоритмы. Симметричные алгоритмы бывают блочными и потоковыми. К блочным шифрам относятся такие алгоритмы: AES, DES, CAST и другие. К потоковым шифрам относятся алгоритмы: RC4, SEAL, WAKE, и, так же, другие алгоритмы.

В этом исследовании были реализованы такие симметричные алгоритмы шифрования, как: AES, DES, RC4. При исследовании такой реализации этих элементов, выявилось, что самым быстрым алгоритмом оказался блочный алгоритм DES, после него, по скорости выполнения оказался потоковый алгоритм RC4, и, на последнем месте оказался блочный алгоритм AES.

Таким образом, симметричные алгоритмы являются довольно быстрыми и простыми в реализации алгоритмами шифрования. Главным существенным минусом таких алгоритмов является сложность обмены ключами, так как для применения необходимо решить проблему надёжной передачи ключей.

УДК 519.688

ПРОГРАМНЕ ДОДАВАННЯ ЛАНЦЮГІВ ПАКЕТУ БАЙТІВ ЧИСЕЛ ЗІ ЗНАКОМ

Третяк І.Р., студент ОТ-315 гр.
Науковий керівник: Бездітко О.М.
Харківський радіотехнічний технікум

Базова система команд передбачає додавання байті, слів, подвійних слів. Тому ланцюги байтів повинні додаватися у програмному циклі пакетом по чотири, два, один байти, починаючи від молодших розрядів та з урахуванням вхідного перенесення. Безумовно, вхідне перенесення зберігається в прапорі CF та є станом збереження вихідного перенесення від попереднього програмного циклу формування суми. При N кількості байтів у ланцюговій послідовності, яка складає операнд зі знаком, легко знайти параметри M = N div 4, L = N mod 4,

де: M – число елементів пакету ланцюга у чотири байти;

L – остача від ділення, що є числом множини 0 .. 3.

Формат числа складається з пакету M по чотири байти, у голові якого можуть знаходитися L байтів. Загальна кількість байтів складає величину N. Такий формат представлення дозволяє укласти вісім варіантів існування числа, чотири із яких мають у хвостовій частині пакет M, а інші чотири не мають. У голові формату можуть бути L байтів (три, два чи один байти) або усі три відсутні. Знаковий біт знаходиться в старшому розряді головного старшого байту.

Алгоритм забезпечує пошук кількості байті у голові ланцюга. Нагадую, їх може бути у межах множини 0 .. 3. Ця величина задається директивно перед виконанням програми. По закінченню програми додавання подвійних слів прапори перенесення і переповнення зберігаються у стеку з метою їх виростання при подальших обчисленнях.

Повідомлення про наявність чи відсутність переповнення розрядної сітки за ознакою програмного тестування прапора переповнення OF стверджує істину про хибність чи істинність результату додавання. Для усунення причини переповнення розрядної сітки необхідно голову ланцюга доповнити байтом зі значенням знакового розширення.

УДК 519.683

КОМП'ЮТЕРНИЙ МОНІТОРИНГ ПРОГРАМНОЇ ЕМУЛЯЦІЇ ДОДАВАННЯ РЕАЛЬНИХ ЧИСЕЛ ПОДВІЙНОЇ ТОЧНОСТІ

Шулінус О.А., студент ОТ-315 гр.,
Науковий керівник: Бездітко О.М.,
Харківський радіотехнічний технікум

Програмне комп'ютерне обчислення суми реальних чисел є досить простою процедурою, якщо дивитися на це з позиції можливостей комп'ютера. Для реалізації цієї задачі обчислювальні потужності комп'ютера значно перевершують межу виконання подібних розрахунків. Таке обчислення уже закладено в комп'ютер та є резидентним і виконується одним простим математичним оператором додавання, яке б це не було програмне мовне середовище. Але річ в іншому, в деталізації послідовних обчислювальних реакціях процесора на виконання елементарних обчислень, з яких складається алгоритм. Така задача вирішується тільки після отриманих глибоких знань по питанням складностей архітектори комп'ютера та надбаного досвіду мистецтва програмування.

Цінність висвітлень оригінальної розробки полягає в пов'язанні авторських теоретичних тлумачень з комп'ютерною практичною реалізацією поставленого алгоритму. Робота користувача з утвореним пакетом програмного забезпечення та цією методичною розробкою розширює кругозір читача та уможливлює спрощення шляхів надбання досвіду особистістю в області програмування. Ця розробка не є подачею теоретичного матеріалу для його вивчення, вона стала основою для будови оригінальних алгоритмів та реалізації комп'ютерних програм. Реалізований алгоритм додавання змінних типу Double з одного боку є стандартним, а з іншої сторони він оригінальний. На відміну від змінної Single, яка має родинні стосунки з попередньою та пов'язаною з батьківською спадщиною від співпроцесора, комп'ютерна програма емуляції додавання чисел подвійної точності більш складна.

Розробка пропонується для запровадження в навчальний процес з підготовки фахівців комп'ютерної направленості.

УДК 004.042

МНОГОПОТОЧНОСТЬ В WPF

Сушинський В.В., студент 515ст2 гр.,
Научный руководитель: к.т.н., доцент Шостак А.В.,
Национальный аэрокосмический университет
им. Н.Е. Жуковского «ХАИ»

WPF поддерживает модель однопоточного апартамента (single-threaded apartment – STA), которая очень похожа на ту, что используется в приложениях Windows Forms. С этой моделью связано несколько основных правил:

– объект WPF обладают потоковой наследственностью (thread affinity). Поток, который создает их, владеет ими, и другие потоки не могут взаимодействовать с ними напрямую.

– объекты WPF, обладающие потоковой наследственностью, наследуются от DispatcherObject в некоторой точке их иерархии классов. DispatcherObject включает небольшой набор членов, которые позволяют верифицировать, выполняется ли код в правильном потоке, чтобы использовать определенный объект, и переключаться на другой поток.

– один поток выполняет все приложение и владеет объектами WPF. Хотя можно использовать отдельные потоки, чтобы отображать отдельные окна, такое проектное решение встречается редко.

Диспетчер управляет работой, происходящей в WPF-приложении. Диспетчер владеет потоком приложения и управляет очередью элементов работы. Во время работы приложения диспетчер принимает новые запросы работы и выполняет их по одному.

Формально диспетчер создается при первоначальном создании в новом потоке экземпляра класса, который наследуется от DispatcherObject. В случае создания отдельных потоков и использования их для отображения отдельных окон получается более одного диспетчера. В данной работе предлагается использовать один поток пользовательского интерфейса и один диспетчер. Затем использовать многопоточность для управления операциями с данными и другими фоновыми задачами.

УДК 004.588

ПРОГРАММА ДЛЯ ПОСТРОЕНИЕ ГРАФИКОВ ФУНКЦИЙ

Судаков Д.А., студент 525б гр.,
Научный руководитель: к.т.н., доцент Шостак А.В.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Разработка обучающего программного обеспечения является неотъемлемой частью развития современных IT технологий. Сейчас трудно представить школу или высшее учебное заведение без компьютеров или проекторов, или другого технического обеспечения. Каждый учитель или преподаватель старается сделать все возможное для большего усвоения знаний учениками, поэтому прибегают к различным методам наглядного представления какой-либо информации.

Целью данной работы является реализация прикладной программы по построению графиков функций на языке C# с использованием среды разработки Visual Studio 2017.

В разрабатываемой программе можно выбрать один из десяти стандартных графиков, задать параметры и шаг изменения по аргументу, изменить цвет построенного графика.

Программные продукты данного назначения широко используются в сети Интернет, но, как правило, реализованы с использованием WPF или Web-технологий.

Программа, разрабатываемая в рамках данной работы, реализуются в виде оконного приложения с использованием графического режима вывода информации на экран. Для визуального представления графиков функций используется компонент Chart, входящий в состав Visual Studio 2017.

В дальнейшем планируется усовершенствование данной программы, а именно ручной ввод любой функции, выбор графика с его параметрами из файла, добавить построение линий тренда (аппроксимация, сглаживание).

УДК 004.421.2

ПОСТРОЕНИЕ ЛАБИРИНТОВ С ПОМОЩЬЮ АЛГОРИТМА ЭЛЛЕРА

Шорский А.Э., студент 525и гр.
Научный руководитель: ст. преподаватель Дужая В.В.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

В настоящее время лабиринты используются в различных сферах деятельности человека. Но наиболее популярной является сфера информационных технологий, в частности, в некоторых видах игр развлекательного жанра. В XXI веке все передовые компании по разработке ПО мира борются за ресурсы компьютера. Чем меньше требует ПО ресурсов, тем лучше.

Целью данной работы является построение односвязного лабиринта, используя минимальное количество ресурсов компьютера. Для достижения этой цели было принято решение использовать алгоритм Эллера. Его принцип работы следующий: создаётся строка с ячейками, каждая из которых принадлежит разным множествам. Далее, двигаясь по этим ячейкам, случайным образом решаем добавить ли стенку справа. Каждая последующая строка строится на основании предыдущей.

На данный момент существует множество разных алгоритмов для построения лабиринтов. Самые известные из них - это алгоритмы двоичного дерева, «Sidewinder», Прима, Краскала и другие.

Проведённый анализ показывает, что алгоритм Эллера работает очень эффективно, даже не смотря на изначально заданную большую размерность лабиринта. В результате работы алгоритма мы получаем односвязный лабиринт, в котором между любыми двумя его клетками существует путь, и притом единственный.

Таким образом, алгоритм позволяет построить лабиринт достаточно большого размера в очень короткие сроки, и при этом используя минимум ресурсов компьютера.

УДК 004.056.55:004.274

РАЗРАБОТКА ОЧЕРЕДИ С ПРИОРИТЕТОМ

Цокота Я.В., студент 525 гр.,
Научный руководитель: к.т.н., доцент Шостак А.В.
Национальный аэрокосмический университет
им. Н.Е. Жуковского «ХАИ»

Одними из важнейших процедур обработки структурированной информации является поиск. Важно выбрать тот алгоритм, который лучше подходит для решения конкретной задачи.

Целью данной работы является разработка системы, которая бы реализовала такую структуру данных, как очередь с приоритетом. Основными операциями над приоритетной очередью являются:

– ВСТАВИТЬ в множество новый элемент со своим ключом.

– НАЙТИ в множестве элемент с минимальным ключом. Если элементов с минимальным ключом несколько, то находится один из них. Найденный элемент не удаляется из множества.

– УДАЛИТЬ из множества элемент с минимальным ключом. Если элементов с минимальным ключом несколько, то удаляется один из них.

Приоритетная очередь естественным образом используется в таких задачах, как сортировка элементов массива, поиск во взвешенном неориентированном графе минимального остовного дерева, поиск кратчайших путей от заданной вершины взвешенного графа до его остальных вершин, и во многих других.

Приоритетную очередь можно представить с помощью массива или списка элементов, но такие реализации неэффективны по времени выполнения основных операций. Так, например, поиск элемента с минимальным ключом в неупорядоченном массиве или списке требует последовательного просмотра всех его элементов. Если поддерживать упорядоченность массива или списка по ключу, то «неудобной» окажется операция вставки нового элемента.

В работе на языке C# было выполнено сравнительное исследование эффективности очереди с приоритетом, реализованной с использованием бинарной и фибоначчивой куч, узлами которых являются обьекты с ключами целочисленного типа.

УДК 004.652:004.657:004.658

ДОСЛІДЖЕННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ РОБОТИ РЕЛЯЦІЙНИХ ТА НЕРЕЛЯЦІЙНИХ БАЗ ДАНИХ НА ПРИКЛАДІ MS SQL SERVER ТА MONGO DB

Саєнко В.А., студент 565аМ гр.,
Науковий керівник: к.т.н., доцент Шостак А.В.
Національний аерокосмічний університет
ім. М.Є. Жуковського «ХАІ»

Вибір правильного типу системи управління базами даних (СУБД) на етапі проектування системи є надзвичайно важливим і повинен враховувати як точне виконання поставлених завдань так і можливість подальшого розвитку системи.

Останнім часом все більшу популярність здобувають системи управління базами даних NoSQL, які мають низку відмінностей від устрою реляційних баз даних, що вже стали класичним варіантом для вирішення задач збереження інформації.

Метою даного дослідження є аналіз та дослідження ефективності роботи реляційних та нереляційних баз даних на прикладі MS SQL Server та Mongo DB. Для досягнення поставленої мети потрібно порівняти принципи побудови баз даних, методики виконання операцій, час виконання цих операцій, а також визначити вразливі місця при роботі з кожною СУБД. Для отримання вірних результатів аналіз проводиться з базами даних однієї і тієї ж логічної структури.

На даний час існує багато джерел інформації по темі дослідження, головними з яких є офіційні веб-сайти СУБД, де інформація оновлюється згідно появи нових версій продуктів.

Проведений аналіз показує, що MS SQL Server та Mongo DB мають різницю в моделі зберігання даних, схемі даних, принципі масштабування, забезпеченні надійного збереження даних, часу виконання запитів. В той же час кожна з цих СУБД переваги, які можуть надати програмі, що розробляється, гнучкості, надійності, продуктивності, швидкості.

Отримані результати можуть бути використані для формування рекомендацій щодо вибору типу СУБД для вирішення поставленої задачі.

УДК 004.05

РАЗРАБОТКА И ИССЛЕДОВАНИЕ МЕТОДИКИ ОЦЕНИВАНИЯ КАЧЕСТВА СИСТЕМ ОТСЛЕЖИВАНИЯ ОШИБОК

Кальницкий М.Э., студент 565аМ гр.,
Научный руководитель: к.т.н., доцент Орехов А.А.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

В современном IT обществе существует множество проектов разной направленности и форматов. Практически во всех проектах используются системы отслеживания ошибок как инструмент организации, распределения и управления ошибками.

Целью данного исследования является разработка методики оценивания систем отслеживания ошибок для выбора наиболее подходящей под определенный проект. Для достижения поставленной цели необходимо решить задачу по выбору определенных параметров системы отслеживания ошибок в соответствии с заданным проектом.

На данный момент существует много различных систем отслеживания ошибок. Например, система Mantis является бесплатной и обладает небольшим функционалом для занесения, хранения и управления ошибками. Данная система может подойти для небольших проектов, не требующих дополнительного функционала для управления персоналом и ролями в системе разработки. В то же время Jira обладает широким набором функционала, позволяющим полностью организовать на базе данной системы отслеживания ошибок процесс разработки, а не только контроль и ведение ошибок.

Проведенный анализ показывает, что оценка качества системы отслеживания ошибок необходима для максимально эффективного и удобного управления не только ошибками, но и проекта в целом.

Анализ качества систем отслеживания ошибок позволит эффективно выбирать подходящую под нужды и реалии проекта систему. Планируется разработка инструментального средства для автоматизации и поддержки процесса оценивания систем отслеживания ошибок.

УДК 004.056.55:004.274

РАСПРЕДЕЛЕННАЯ СИСТЕМА МОНИТОРИНГА НА ОСНОВЕ БПЛА

Тихонов А.В., студент 565аМ гр.,
Научный руководитель: доцент Плахтеев А.П.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Современные системы: промышленного, экологического, сельскохозяйственного мониторинга отличаются большими областями покрытия требованием уменьшение стоимости развертывания и эксплуатации. Это требует использования мобильных элементов (автономные наземные платформы, БПЛА) объединенных мобильными сетями с доступом к интернету и облачным сервисам.

Цель данной работы является разработка сетевой инфраструктуры для распределенной системы мониторинга схемы взаимодействия с инфраструктурой. В работе решаются задачи увеличения времени автономной работы способов и видов безопасного обмена, данных приемо-передачи между инфраструктурой и квадрокоптерами.

Квадрокоптеры ведущих производителей – Aeryon Systems, Draganfly, Idea-Fly имеют полезную нагрузку до 3-5 кг также каналы управления и передачи данных на расстояние 500м -1км.

Для расширения области мониторинга может использоваться множество квадрокоптеров объединенных в мобильную сеть. Для максимальной эффективности работы системы в целом нужно предусмотреть надежную связь, бесперебойное питания, реализацию шифрование данных, способы подзарядки квадрокоптеров, способы и виды передачи данных между станциями и квадрокоптерами, так же возможность получать и обрабатывать предаваемую информацию в реальном времени.

Инфраструктуры мониторинга на основе квадрокоптера позволяет решить многие проблемы в получение информации и контроля в труднодоступных мест.

UDC 004.4'2

IOT SOLUTIONS FOR HEALTH MONITORING: ANALYSIS AND CASE STUDY

Medvediev Ivan., Student of group 555vM,
Scientific advisor Uzun D.D.,
National Aerospace University named
after N.E. Zhukovsky "KhAI"

Motivation. The IoT is one of the newest and most promising trends in the healthcare industry. Recent advances in health, microelectronics and sensor manufacturing, and data processing and storage have made it possible to change the approach for developing complexes for healthcare to a new level. Due to the complexity, multilayeredness and hierarchy of healthcare IoT systems personal data about human condition is of very sensitive asset, so there are problems of privacy and security of such systems should be resolved.

Goal. The paper considers the analysis and comparison of hardware and software solutions for creating a device and service for monitoring of the patient's health based on an electrocardiograph.

The advantage of this study is the use of hardware and technology platforms that were not used previously for similar purposes. For the purposes of interaction with cloud services and for more convenient development and debugging processes an open source and free software tools are used. As components for the assembly of the device the modern technical equipment which exists on the market is considered. The practical implementation of the device as well as the modeled service infrastructure is provided.

Results. In the article the existing hardware and software components for the construction of medical solutions using IoT platform and cloud service were analyzed. The rationale for their choice is provided. Particular attention was paid to security and privacy. In particular, the hardware module for a secure connection to the cloud service have been developed. The cloud service was selected taking into account the requirements of the Health Insurance Portability and Accountability Act (HIPAA).

Designed prototype with its implemented functionality can compete with professional instruments for measurement of ECG, albeit at a much cheaper price.

УДК 004.716:621.391

АНАЛИЗ ВАРИАНТОВ МАРШРУТИЗАЦИИ УПРАВЛЯЮЩИХ СИГНАЛОВ В БЕСПРОВОДНЫХ СЕТЯХ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ УПРАВЛЕНИЯ ИСПОЛНИТЕЛЬНЫМИ УСТРОЙСТВАМИ УМНОГО ДОМА

Косаревский Б.В., студент 568М гр.,
Научный руководитель: к.т.н., доцент Абрамов С.К.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

В настоящее время актуальна задача передачи и маршрутизации управляющих сигналов в сетях управления умным домом. В работе предлагается анализ существующих протоколов, применяющихся при построении умного дома или использовании средств автоматизации управления различными исполнительными устройствами.

Целью данного исследования является выбор протокола, позволяющего решить задачу передачи и маршрутизации сигналов управления при учёте следующих основных требований: независимость от существующих сетей (в том числе IP), максимальная отказоустойчивость (ячеистая топология сети).

Были рассмотрены 7 протоколов: 1-Wire, X10, KNX, Wi-Fi, ZigBee, Z-Wave, Insteon. Ввиду того, что необходимо оказывать минимальное влияние на существующую сетевую структуру здания, было принято решение отказаться от использования кабельной среды передачи данных. Wi-Fi и прочие протоколы использующие частоту 2,4 ГГц не соответствуют требованию о независимости от существующих сетей (к тому же, при работе в данном диапазоне частот возможны помехи для существующих Wi-Fi сетей). KNX и Insteon используются очень редко. ZigBee имеет недостаточный уровень стандартизации и является закрытым. Также маршрутизаторы ZigBee имеют повышенные требования к питанию.

В результате проведенных исследований было предложено использовать протокол Z-Wave, который лишен перечисленных недостатков, имеет строгий уровень стандартизации и позволяет решить поставленную задачу в полном объеме.

УДК 004.4: 628.93

РАЗРАБОТКА ПРИЛОЖЕНИЯ БЕСПРОВОДНОГО УПРАВЛЕНИЯ СВЕТОДИОДНОЙ ЛЕНТОЙ С ПИКСЕЛЬНОЙ АДРЕСАЦИЕЙ

Землянко Г.А., студент 545 гр.,
Научный руководитель: к.т.н., доцент Плахтеев А.П.,
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Данная работа посвящена актуальной теме использования мобильных устройств с технологией Bluetooth для связи с устройством управления светодиодной лентой с пиксельной адресацией для учебных и демонстрационных целей. Предполагается управление яркостью, установление цветовой палитры, реализация динамических функций светодиодной ленты.

Взаимодействие смартфона со светодиодной лентой осуществляется с помощью приложения, которое было разработано для Android, которое обеспечивает связь с Bluetooth модулями HC-05. Данная программа предоставляет специальную работу со светодиодной лентой и управление ею.

Таким образом, мобильное приложение с данным модулем беспроводного управления светодиодной лентой с пиксельной адресацией, разработанное для учебных и демонстрационных целей позволяет познакомиться с технологией беспроводного управления светодиодной ленты. В дальнейшем планируется модернизировать приложение, добавить управление несколькими модулями и светодиодными лентами, возможность управлять одним пикселем ленты. У пользователя будет возможность получать информацию о модулях, какими лентами управляет данный модуль. Разработается функция удаления и добавления необходимых модулей, если будет необходимость их заменять. Появиться функция получения доступа к управлению определенным модулем. Так же планируется разработать собственное приложение на IOS; исследовать устойчивость управления к DDoS-атакам и способы повышения безопасности; определить дальность передачи Bluetooth-сигнала и снизить его энергопотребление.

УДК 004.4: 628.973.1

РАЗРАБОТКА МОДУЛЯ БЕСПРОВОДНОГО УПРАВЛЕНИЯ СВЕТОДИОДНОЙ ЛЕНТОЙ С ПИКСЕЛЬНОЙ АДРЕСАЦИЕЙ

Хебнев А.В., студент 545 гр.,
Научный руководитель: к.т.н., доцент Плахтеев А.П.,
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Актуальным является как разработка контроллеров для светодиодных лент, так и приобретение навыков интерактивного взаимодействия с «умным» освещением посредством мобильных устройств. Данная работа посвящена разработке программно-аппаратных средств прототипа модуля управления через Bluetooth 3.0 светодиодной лентой WS2812B с пиксельной адресацией для учебных и демонстрационных целей.

Анализ существующих решений показывает, что для решения этой задачи достаточно 6 - 8 кб памяти программ. Принято решение использовать малогабаритное микроконтроллерное устройство Arduino mini, которое обеспечивает управление светодиодными лентами WS2812B , где каждый пиксель имеет 3 излучающих светодиода (красный, синий и зеленый) и встроенные 8- битные ШИМ-драйверы, управляющие их яркостью. Из Bluetooth модулей выбран HC-05, поскольку он является одним из самих распространенных и имеет малую стоимость.

В результате работы был создан прототип модуля управления одиночной светодиодной лентой на основе технологии Bluetooth 3.0. В дальнейшем планируется разработать подробное руководство пользования данным устройством. Для дальнейшей разработки была поставлена задача расширения возможностей микроконтроллера для управления лентой. Для её решения будет реализовано добавление новых команд, что позволит увеличить количество лент и управление ими. Также планируется добавить команду, которая позволит пользователю управлять отдельным пикселем, а именно: выбор позиции, цвета и интенсивности излучения. Будет предусмотрено управление группой пикселей светодиодных лент, если они находятся на расстоянии друг от друга. Требуется разработать способы повышения безопасности и надежности устройства.

УДК 004

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ РОЗВИТКУ МОБІЛЬНОГО ІНТЕРНЕТУ ПОКОЛІННЯ 3G. РОЗРОБКА ВЛАСНОЇ ПРОГРАМИ «BNG» ДЛЯ КРАЩОГО ПОШИРЕННЯ СИГНАЛУ

Бєлінський Р.А., учень 11-А класу
Науковий керівник: учитель інформатики Єфімова Я. В.
Комунальний заклад «Обласна спеціалізована школа-інтернат II-III ступенів «Обдарованість» Харківської обласної ради»

Сучасний стан аналізу використання мобільного інтернету свідчить про нерівномірність розподілу сигналу 3G та включає можливість використання всіма бажаючими. Основною причиною такого розподілу є не низьке матеріально-технічне забезпечення розвитку цієї технології, а нераціональне використання.

З усього вищезазначеного можна зробити висновок про необхідність пошуку шляхів вирішення питання поширення та якісного забезпечення 3G більшої території. Актуальність роботи полягає в тому, що потрібно дослідити дійсний стан та особливості поширення 3G сигналу, проаналізувавши карти основних постачальників цієї технології в Україні.

Об'єктом дослідження є процес власної реалізації програми «BnG», яка дозволить визначити мінімальні затрати для поширення 3G.

Предметом в науковій роботі є дослідження шляхів поширення мобільного інтернету, детальне вивчення аспектів його започаткування та використання 3G технологій.

Метою роботи є проведення всебічного аналізу, вирішення проблеми покращення та доступності сигналу 3G у всі точки нашої країни. Значною частиною роботи є розробка програми «BnG» для якіснішого забезпечення сигналу.

Завдання роботи, за допомогою яких буде втілена мета: вивчити проблеми та загальні відомості про сучасний стан технологій поширення мобільного інтернет-сигналу; визначити оптимальні напрямки та запропонувати раціональні рішення цього питання; деталізоване проектування структури проекту, його покроковий опис та внесення підсумкових коригувань; вибір інструментів та засобів реалізації програми.

УДК 004.35

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ТЕХНОЛОГИИ INTERNET OF THINGS

Новоспасский А.С. ученик 10-А класса,
Научный руководитель: ассистент кафедры 503 Егорова Е.В.,
Аэрокосмический лицей на базе НАУ «ХАИ»

Для начала, следует понимать, что же такое Интернет вещей, и почему же он актуален сейчас. Итак, Интернет вещей это такая вычислительная сеть физических предметов, которая охватывает практически все сферы деятельности человека, начиная от быта и заканчивая отраслями промышленности. Эта технология может решить некоторые глобальные проблемы человечества, именно поэтому сейчас она и актуальна.

Цель этой сети состоит в том, чтобы значительно трансформировать личные и социальные аспекты жизни человека. Самыми примитивными примерами этого явления являются умные часы, умный дом, умный чайник и т.п.

Сейчас существует несколько препятствий на «пути» распространения IoT. Первый минус IoT это низкий уровень безопасности. Согласно исследованиям, до 80% устройств будут уязвимы извне. Однако я считаю, что это лишь вопрос времени. Так же существует проблема энергопитания подключенных устройств. Многие из этих устройств - различные беспроводные сенсоры и датчики. Таковых будет размещено огромное количество, в том числе и в труднодоступных местах, и затраты на замену в них элементов питания могут свести на нет все выгоды от их использования. И последняя, самая сложная преграда для преодоления – психологическая. Она состоит в том, что многие потребители не готовы впустить к себе в жизнь умные устройства по различным причинам. Многие же просто считают, что умные вещи не создают добавленной стоимости, бесполезны и дороги.

На мой взгляд, согласно темпам роста популярности Интернета вещей за последние несколько лет, можно однозначно сказать, что IoT – достаточно перспективная технология, которая уже через пару лет сможет стать повсеместной и востребованной в быту, а так же в любой отрасли промышленности.

УДК 004.056.55:004.274

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ БЕСПИЛОТНЫХ АППАРАТОВ

Товкало Е.П., Хапокныш Ю.В., студент 525-А гр.,
Научный руководитель: к.т.н., доцент Шостак А.В.
Национальный аэрокосмический університет им. Н.Е. Жуковского «ХАИ»

На сегодняшний день все большую популярность приобретает идея беспилотных аппаратов, как летательных, так и наземных. Многие компании уже представили свои концепты и модели легковых автомобилей, грузовиков и вездеходов способных передвигаться без присутствия водителя в кабине. Не менее активно подобные машины используются для научных и военных целей, а также для проведение спасательных операций.

Данная работа направлена на анализ перспектив использования беспилотной техники в разных отраслях и сферах жизни человека. Для этого мы изучим существующие разработки, оценим результаты их работы и проведенных ранее испытаний.

Потенциал беспилотного транспорта позволяет трансформировать нашу цивилизацию в масштабах, невиданных с тех пор, как автомобили, потеснив лошадей, обрели статус главного транспортного средства человечества. Основные работы ведутся над улучшением алгоритмов глубокого обучения.

Изучив возможности уже существующих и разрабатываемых моделей, становится понятно, что область применения данных технологий намного шире, чем пассажирские перевозки и доставка грузов. Самоуправляемые авто будущего окажутся существенно более эффективными и безопасными, а это подразумевает снижение уровня смертности в ДТП и остроты проблемы пробок, а также уменьшение потребления энергоносителей. Подобные машины могут стать надежными помощниками в научных исследованиях и при тушении пожаров.

Беспилотные аппараты безусловно создаются с целью обезопасить нашу жизнь, уменьшив количество аварий на дорогах, заменяя людей во время устранения последствий разного рода катастроф и снижая риски при исследовании труднодоступных участков нашей планеты.

УДК 338.28:711:629.735.7

МОНИТОРИНГ С ИСПОЛЬЗОВАНИЕМ КВАДРОКОПТЕРОВ В СОСТАВЕ ПРОЕКТА SMART CITY

Чуйко А.А., Гулий В.В., студент 515 ст1 гр.,
Научный руководитель: ст. преподаватель Перепелицын А.Е.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

В настоящее время всё больше набирает популярность система «Умный город», а именно системы отслеживания преступности и видеонаблюдения. Для решения данной проблемы предлагается система отслеживания с помощью квадрокоптеров. Также данный вид устройств может найти применение в консультации граждан, по средствам аудио-видео информирования, в сфере оказания первой доврачебной помощи, что позволит существенно повысить шансы на благополучный исход пострадавшего.

Целью данного исследования является повышение безопасности людей в городской среде. Для достижения поставленной цели необходимо провести анализ производительности и требуемого количества ресурсов для мультикоптера, а также решить задачу организации связи на больших расстояниях.

Проведенный аналитический обзор существующих решения показывает, что существующие системы, такие как система умного видеонаблюдения Smart cities, имеют ряд ограничений, связанных с технической реализацией: ограниченный угол обзора, статичное расположение камер и наличие «слепых» зон.

Проведённый анализ показывает, что применение квадрокоптера для решения данной задачи требует от аппарата маневренности и мобильности в условиях городской среды. Также для максимальной эффективности работы необходимо предусмотреть прямую связь на больших расстояниях с использованием беспроводных GSM технологий и программы управления на компьютере диспетчера.

Таким образом, квадрокоптеры должны найти свою нишу в мониторинге и устранении чрезвычайных ситуаций. Проект будет представлять собой «улей» дронов, расположенных по районам городов, с единым диспетчерским центром.

УДК 004.42:004.75

АНАЛИЗ ПРОГРАММНЫХ СРЕДСТВ ПОВЫШЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ КЛИЕНТСКОЙ ЧАСТИ WEB-ПРИЛОЖЕНИЙ

Москаленко Б.В., студент 565аМ гр.,
Научный руководитель: ст. преподаватель Перепелицын А.Е.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

В настоящие время наблюдается рост востребованности разноплановых web-приложений, позволяющих быстро получать информацию. К их числу также относятся новостные ленты, содержащие новейший контент о последних событиях, происходящих в мире. Другие ориентированы на предоставление сервисов общения, совершения покупок через интернет и поиска информация для обучения. Повышение спроса на такие решения формирует новые требования к разработчикам, в том числе и в аспекте производительности web-сервиса.

Целью данной работы является повышение производительности web-приложений. Для достижения поставленной цели необходимо решить задачу анализа и систематизации средств оценки и повышения производительности web-приложений.

Большие и средние компании, которые заботятся о качестве и производительности своих web-приложений зачастую имею свой стек утилит для определенных технологий, которые они используют при разработке. Проведенный анализ позволил определить простые методы и способы для увеличения производительности разрабатываемого приложения. Были рассмотрены утилиты для минимизации исходного кода приложения, оптимизации изображений и шрифтов. Так же были рассмотрены рекомендации по оптимизации кода клиентской части веб-приложения, что дало не малый прирост в производительности.

Таким образом, при выполнении рефакторинга, минимизации исходного кода клиентской части приложения, оптимизации ресурсов, которые используются приложением, получается достичь полуторакратного прироста произвольности в сравнении с исходной скоростью загрузки. Этот результат позволяет повысить удобство эксплуатации таких сервисов.

УДК 004.056.55

МОДЕЛЬ КРИПТОПРЕОБРАЗОВАНИЯ ДАННЫХ ПО СХЕМЕ ЗАДАЧИ О РЮКЗАКЕ НА ОСНОВЕ ПРИНЦИПА ДИВЕРСНОСТИ

Нос Р. С., студент 565аМ гр.,
Научный руководитель: к.т.н., доцент Лысенко И. В.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Задача обеспечения конфиденциальности данных, передаваемых по незащищённым каналам, до сих пор является актуальной. Наибольшую популярность приобрели RSA- и El Gamal-подобные криптоалгоритмы. В то же время, не прекращаются попытки модернизировать алгоритм на основе задачи о рюкзаке.

Целью данной работы является описание подхода, основанного на принципе диверсности, позволяющего, как предполагается, повысить криптостойкость и свести к минимуму угрозу встраивания в алгоритм секретных лазеек, на примере криптоалгоритма на базе классической схемы задачи о рюкзаке.

Ранее уже были предприняты попытки модификации рассматриваемого алгоритма с использованием китайской теоремы об остатках, на базе алгебраической теории кодирования, с использованием принципа мультипликативного рюкзака, методом фиксирования рюкзачного вектора для каждого этапа, на основе диофантовых уравнений и др.

В общем виде идея предлагаемого подхода заключается в предоставлении разработчиком криптосистемы генерировать множество сверхвозрастающих рюкзаков, которые могли бы использоваться для шифрования и расшифрования разных блоков одного сообщения неизвестным ни для кого образом.

В результате анализа было выявлено, что недостатком подхода является увеличение ключевого материала и некоторое увеличения времени криптопреобразования в сравнении с реализацией классической схемы рюкзачной криптосистемы.

Таким образом, предложенный подход позволяет снизить риски неконтролируемых ситуаций, связанных с возможностями разработчиков встраивать секретные лазейки в схемы генерации ключей криптоалгоритмов.

УДК 004.4'2

РАЗРАБОТКА И ИССЛЕДОВАНИЕ ИНСТРУМЕНТАЛЬНОГО СРЕДСТВА ДЛЯ ОЦЕНКИ СТАРТАП-ПРОЕКТОВ

Почернин А.М., студент 565аМ гр.,
Научный руководитель: к.т.н., доцент Узун Д.Д.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Данная тема является актуальной, т.к. на сегодняшний день начинающие проекты имеют широкое распространение. Для повышения вероятности успеха проекта необходимо исследовать рынок, определить наиболее актуальные отрасли для развития, выявить тренды на рынке и потребности клиентов.

Как показывают исследования, рынок стартапов постоянно развивается и все прочнее закрепляется как возможность молодым разработчикам предложить свои наработки и идеи. Основными проблемами развития стартап проектов являются поиск средств на реализацию проекта, а так же реализация своих идей в актуальных трендах. Нередко хорошая идея может быть не реализована или может не получить необходимую поддержку со стороны потенциальных потребителей. На сегодняшний день существуют системы краудфандинга, позволяющие решить проблему поиска средств для реализации стартап идеи. Такие системы позволяют демонстрировать существующие наработки по проекту, что в свою очередь помогает находить потенциальных потребителей продукта, которые материально помогают разработчикам для запуска их проекта. Но проблема выявления трендов развития остается актуальной. Частично ее решает «Метода Анализа Иерархий», успешно зарекомендовавший себя как математический инструмент системного подхода к сложным проблемам принятия решений

В результате исследований проанализированы преимущества и недостатки существующих систем краудфандинга. Предложен способ улучшения систем краудфандинга путем внедрения инструмента для выявления трендов направлений развития проектов в зависимости от запросов потенциальных бизнес-инвесторов. Такой инструмент позволит увеличить вероятность коммерческого успеха для стартап проекта.

УДК 004.056.52

ИССЛЕДОВАНИЕ И РАЗРАБОТКА МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ В КОНТЕКСТЕ ЗДРАВООХРАНЕНИЯ

Андрийчук А.С., студент 565вм гр.
Научный руководитель: к.т.н. Узун Д.Д.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

На сегодняшний день, медицина является одной из сфер услуг, которая на наших глазах переходит в цифровой мир. Бумажные данные, занимавшие несколько комнат, теперь умещаются в кармане, а доступ можно получить из любой точки земного шара, с помощью приложения. Это одна из сфер применения, где конфиденциальность, целостность доступность, данных стоит выше, чем дизайн или интерфейс приложения. Для обеспечения безопасности данных пациентов необходимо тщательно разработать модель доступа к данным основываясь на международных стандартах.

Целью данного исследования является создание политики безопасности на основе ролей, которая определяет потоки информации, разрешенные в системе, основываясь на международных стандартах HIPAA и GDPR.

На данный момент существует несколько проектов занимающиеся реализацией доступа к данным. Один из них – HIPAAShield, суть которого состоит в документации формальных требований, предъявляемых к системе. Так же, хотелось бы отметить компанию HIPAA Academy, которая предоставляет готовый модуль управления данными.

Проведённое исследование показало, что разрабатываемая модель дожна опираться на существующие стандарты защиты PHI, обладать свойствами абстрактности и простоты, а так же не накладывать ограничений на реализацию других механизмов защиты.

Таким образом, разработання модель позволяет решить задачу информационной безопасности в медицине. На данный момент она используется на нескольких медицинских порталах в США.

УДК 004.352.2

RFID СКУД С ИСПОЛЬЗОВАНИЕМ СЕТЕВЫХ ТЕХНОЛОГИЙ

Павлюков Е.А., студент 565 иМ гр.
Научный руководитель: доцент Плахтеев А.П.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Системы контроля и управления доступа (СКУД) находят широкое применение в современных офисах. Современные СКУД развиваются в направлении интеграции с общей системой безопасности и широкого применения сетевых технологий.

Целью данной работы является улучшение гибкости и масштабируемости СКУД на основе RFID. Для достижения поставленной цели необходимо проанализировать существующие решения, а также решить задачу разработки сетевой СКУД и приложения для администрирования RFID ключей.

На данный момент выделяются множество проектов, таких как СКУД от компании HID Global. И СКУД от российской компании RusGuard. Все эти проекты имеют различное исполнение, однако не обладают достаточной гибкостью и масштабируемостью. В данный момент появляются СКУД на основе облачных сервисов, которые позволяют решить данную проблему.

В данной работе рассмотрен сетевой СКУД на примере плана кафедры. В системе предусмотрено снижение участия человека администрировании большого количества ключей и ограничение доступа к аудиториям согласно учебному плану. Также, для максимальной эффективности работы необходимо предусмотреть обновление данных в реальном времени.

Таким образом, СКУД позволяет решить проблему гибкости и масштабируемости и взаимодействия с системами общей безопасности.

УДК 004.75

АНАЛИЗ ДОРОЖНОЙ ОБСТАНОВКИ И ОЦЕНКА ОПАСНОСТИ НА ДОРОГЕ

Геллер С.И., студент 565м гр.
Научный руководитель: профессор А.А. Орехов
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Обеспечение высокого уровня безопасности транспортных средств является весьма актуальной задачей.

Цель работы – повышение безопасности дорожного движения за счет прогнозирования дорожной обстановки, состояния водителя и транспортного средства, а также своевременного информирования водителей в кооперативных интеллектуальных транспортных системах.

Возможный подход к решению данной задачи – разработка системы принятия решений (СПР). Ключевой задачей СПР является анализ входных данных (информация о состоянии водителя, о состоянии автомобиля, об окружающей среде) и прогнозирование возможных опасных ситуаций. Также система должна формировать дорожную обстановку для каждого участника кооперации.

В данной работе рассматривается метод построения СПР на основе дерева принятия решений. Структура дерева представляет собой «листья» и «ветки». На «ветках» дерева решений записаны атрибуты, от которых зависит целевая функция, в «листьях» записаны значения целевой функции, а в остальных узлах атрибуты, по которым различаются случаи. Чтобы классифицировать новый случай, надо спуститься по дереву до листа и выдать соответствующее значение. Подобные деревья решений широко используются в интеллектуальном анализе данных. Цель состоит в том, чтобы создать модель, которая предсказывает значение целевой переменной на основе нескольких переменных на входе.

Разработана архитектура клиент-серверной системы, в которой на стороне сервера находится система динамической оценки безопасности транспортных средств.

УДК 004.056.5

РЕАЛИЗАЦИЯ ПРОТОКОЛА УПРАВЛЕНИЯ ЭЛЕКТРОННЫМ КЛЮЧЕМ ПО БЕСПРОВОДНОМУ КАНАЛУ СВЯЗИ

Карпенко А.С., студент 555иМ гр.
Научный руководитель: д.т.н., профессор Потий А.В.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

На сегодняшний день использование электронно-цифровой подписи, для предпринимателей, стало уже привычным делом. В классическом варианте для выполнения операций подписи пользователю необходимо иметь: рабочую станцию, специальное программное обеспечение и ключевой носитель. В эре высокой информатизации, где появилось множество устройств с беспроводными приемо-передатчиками, не обладающими портами USB, в результате чего была поставлена задача на исследование, которая заключалась в разработке программно-аппаратного комплекса для управление ключевым носителем под средством беспроводной технологии Bluetooth.

Целью данной работы является создание дополнительного интерфейса взаимодействия для криптографических библиотек электронно-цифровой подписи. Для достижения поставленной цели необходимо произвести анализ библиотек, предоставляющие доступ к Bluetooth на различных операционных системах: Windows, Android, IOS.

Результатом работы является выбор стека Bluetooth, добавление интерфейса Bluetooth для комплекса «ІІТ Користувач ЦСК».

Таким образом добавление нового интерфейса взаимодействия с ключевым носителем позволяет мобильным устройствам получить доступ к ключевой информации.

УДК 004.056

АНАЛИЗ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ ТЕХНОЛОГИЙ

Карпенко А.С., студент 555иМ гр.
Научный руководитель: д.т.н., профессор Потий А.В.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

На сегодняшний день популярность беспроводных сетей возрастает. Это объясняется удобством использования, не надо прокладывать кабельную инфраструктуру, дешевизной и приемлемой пропускной способностью. Принимая во внимание текущую динамику развития, можно сделать вывод: беспроводные сети в скором будущем превзойдут проводные сети. Это развитие влияет и на требования к защите информации в беспроводных сетях.

Целью данной работы является рассмотрение и анализ существующих протоколов беспроводной связи с точки зрения защиты информации. В ходе чего необходимо решить ряд задач: определить перечень беспроводных технологий, выделить функции обеспечения информационной безопасности, проанализировать алгоритмы шифрования и протоколов безопасности.

Проанализированные протоколы беспроводных сетей, в которых используются криптографические алгоритмы и протоколы, не обеспечивают приемлемого уровня безопасности передаваемой информации по беспроводному каналу связи. Это связано с недостаточной криптографической стойкостью алгоритмов шифрования и отсутствием протоколов аутентификации узлов и пакетов.

Таким образом при создании безопасных беспроводных сетей нужно уделить большое внимание к защите данных т. к. из всех рассмотренных протоколов беспроводной связи всего лишь ZigBee, Wi-Fi, WiMax, UWB и Z-wave имеют надлежащие алгоритмы защиты данных стойкие к атаке «грубой силы».

УДК 004.056

АНАЛИЗ STATELESS СХЕМ ЦИФРОВОЙ ПОДПИСИ С УЧЕТОМ КВАНТОВОЙ ЗАЩИЩЕННОСТИ

Карпенко А.С., студент 555иМ гр.
Научный руководитель: д.т.н., профессор Потий А.В.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Цифровая подпись является важным примитивом современной криптографии. Множество протоколов безопасности: SSH, TLS и др.; которые используют цифровую подпись для подтверждения аутентичности и проверки целостности. Но, используемые на сегодняшний день схемы, легко скомпрометировать, использовав программируемый квантовый компьютер, использовав алгоритм Шора. Конечно, квантовый компьютер пока является недостижимым, но мировые организации, такие как NIST и ETSI, уже ведут исследования в этой области. Наиболее перспективным схемами подписи являются схемы на основе хеш функции. Но схемы такие как XMSS, MSS, LMS необходимо сохранять состояние, для того чтобы повторно не использовать уже примененную одноразовую ключевую пару, что является проблемой. Для решение этой проблемы существуют схемы SPHINCS и GRAVITY.

Целью является исследование stateless схем цифровой подписи. Для достижения этой цели необходимо решить ряд задач: определить характеристики схем, произвести исследования стойкости этих схем, проверить возможность использования доказуемо стойких хеш функций.

Проведенный анализ показывает большую эффективность и стойкость stateless схем. Эффективность достигается путем уменьшения параметров схемы без ущерба скорости работы схемы. Стойкость схем, основанных на использовании хеш функции, базируются на криптографически стойких однонаправленных функциях, что позволяет противостоять даже гипотетических атакам.

Таким образом наиболее перспективным направлением развития схем на основе хеш функции, являются stateless схемы.

УДК 57.087.1:004.056.5

БІОМЕТРИЧНІ СИСТЕМИ ЯК ЗАСІБ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ

Бородавка В.В., студент 545-і гр.,
Науковий керівник: ст. викладач Цуранов М.В.
Національний аерокосмічний університет
ім. М.Є. Жуковського «ХАІ»

В будь-якій інформаційній системі надзвичайно важливими є засоби та методи автентифікації користувачів. Традиційні методи персональної автентифікації засновані на застосуванні паролів або матеріальних носіїв, таких як смарт-карта, RFID-мітка, eToken або електронний ключ. Дані методи не відповідають сучасним вимогам безпеки, оскільки пароль досить легко забути або перехопити, а матеріальний носій можна підробити, або втратити. Головним напрямком для вирішення цих проблем є вдосконалення методів автентифікації користувачів за рахунок застосування біометричних технологій, які дозволяють забезпечити доступ до інформаційних систем виключно легітимним користувачам, а також обмежити доступ до інформаційних систем зловмисникам. На даний момент спостерігається тенденція трансформації біометричних технологій в повноцінний компонент систем захисту.

Метою даної роботи є розгляд існуючих біометричних методів, які використовуються для автентифікації користувачів, з розробкою методології вибору засобу автентифікації в залежності від сфери застосування.

Порівняльний аналіз систем біометричної автентифікації є досить складним процесом, тому для отримання об'єктивних результатів були введені різні категорії порівняння. Дані категорії мають шкалу оцінювання від 1 до 10. Оцінювання проводилося методом ранжування з порівняльною оцінкою об'єктів. Після усереднення виставлених оцінок при розрахунках кінцевих результатів враховувався вплив кожної категорії в кінцевій системі за допомогою вагових коефіцієнтів, виставлених згідно методу Черчмена-Акоффа. Дані коефіцієнти дають змогу регулювати сферу застосування біометричних методів автентифікації, а отже і біометричних систем.

УДК 004.658.6

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ ВІД КІБЕРЗЛОЧИНЦІВ

Трегуб Ю.В., студент 545і гр.
Науковий керівник: Цуранов М.В., ст. викладач кафедри 503
Національний аерокосмічний університет
ім. Н. Є. Жуковського «ХАІ»

З розвитком інформаційного суспільства та поширенням використання мережі Інтернет, всі сфери людської життєдіяльності зазнають великих змін. Саме тому світові компанії почали активне впровадження різних онлайн-послуг, які дозволяють користувачам швидко та ефективно взаємодіяти з інформаційними системами. Нещодавно компанія «Київстар» об'явила про запуск сервісу електронної ідентифікації – Mobile ID, для отримання державних та комерційних послуг. Тому, питання захисту даних користувачів постає на перший план. Одним із сучасних методів захисту даних у інформаційних системах є технологія блокчейн.

Блокчейн - це розподілена база даних, яка представляє собою один із способів зберігання, обробки та захисту даних користувачів. Існує два види блокчейну: приватні та публічні. Приватні блокчейни – це блокчейни, в яких використовується технологія «докази роботи» (proof-of-work), де всі права на зчитування/запис належать одній організації. Публічні блокчейни захищаються механізмами криптографічного верифікації (proof-of-stake), де права всіх учасників однакові, що не гарантує повноцінну конфіденційність даних.

На сьогодні ця технологія має широке застосування і дозволяє наблизити онлайн сервіси нашої держави до найвищих стандартів інформаційного суспільства. Завдяки цьому дані користувачів будуть надійно захищені від фальсифікації та несанкціонованого доступу зловмисника.

В результаті проведеного аналізу були запропоновані шляхи впровадження технології блокчейн та обробки даних в державні і комерційні структури. Виявлені недоліки в реалізації технології блокчейн для державного земельного кадастру України, та запропоновані шляхи їх вирішення.

УДК 004.056.55

АЛГОРИТМ ШИФРОВАНИЯ «КУЗНЕЧИК» И СРАВНЕНИЕ ЕГО С ДРУГИМИ СТАНДАРТАМИ БСШ

Дука И.А., студент 525-и гр.,
Научный руководитель: к.т.н., доцент Лысенко И.В.,
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Проблема обеспечения конфиденциальности данных является, как известно, одной из основных в сфере кибербезопасности. Целью данной работы является:

– описание российского блочного симметричного шифра (БСШ) «Кузнечик»;

– программная реализация БСШ «Кузнечик» и сравнение полученных результатов с результатом работы оптимизированной версией, найденной в интернете;

– сравнение БСШ «Кузнечик» с отечественным стандартом БСШ «Калина» и криптоалгоритмом AES, являющимся фактически международным стандартом БСШ.

Была осуществлена программная реализация БСШ «Кузнечик», позволяющая выполнять криптопреобразование документа произвольной длины. Так, шифрование книги объёмом 250 страниц производится за 17,64 сек., т.е. со скоростью 0,319 Mbit/s. Этот результат довольно низкий, если его сравнивать с результатами оптимизированной версии, а именно 1081,08 Mbit/s.

Также, на основании данных, найденных на некоторых Интернет-ресурсах, произведено сравнение БСШ «Кузнечик», «Калина» и AES по показателю быстродействия. В результате сравнения было установлено, что стандарт БСШ «Калина» является наиболее быстродействующим.

Получена таблица, содержание которой позволяет сравнить перечисленные БСШ с точки зрения таких параметров, как: длина ключа, длина блока шифруемых данных, используемая конструкция шифра, число раундов криптопреобразования, используемые базовые криптопримитивы.

УДК 004.852

ЧАСТОТНЫЙ СЛОВАРЬ

Кийко О.Д., студент гр. 525и,
Научный руководитель: ст.преподаватель Дужая В.В.,
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Задача частотного анализа текста находит широкое применение в лингвистике и криптографии. Частотный анализ текста может применяться для определения частоты появления символов в тексте, для определения водности текста и его «тошноты». Также применением частотного анализа может быть вычисление энтропии ключей для определения их надёжности и для попыток расшифровки текста, которые были зашифрованы моноалфавитным шифром простой замены типа афинный шифр Цезаря.

Целью данной работы является разработка программы, которая будет проводить анализ текста, составлять частотный словарь, а так же определять язык для достаточно длинных (от 1000 символов) разнообразных текстов. Выбраны следующие языки: русский, английский, итальянский.

На данный момент для решения задачи частотного анализа текста по буквам существуют несколько проектов, таких как программа на Windows «TextAnalyzator» и интернет-ресурс «Онлайн калькулятор. Частотный анализ текста».

Проведенный анализ показал, что для надёжного определения языка текста необходимо, чтобы размер текста был не менее 1000 символов, текст должен быть разнообразным и осмысленным.

Таким образом, разработанная программа позволяет провести частотный анализ текста и определить язык осмысленного текста. В качестве развития программы может выступать добавления других языков, а так же усовершенствование алгоритмов определения языка и получение различных лингвистических характеристик рассматриваемых языков.

УДК 004.056.55

ПОСТ-КВАНТОВЫЕ АЛГОРИТМЫ ЦИФРОВОЙ ПОДПИСИ ОСНОВАННЫЕ НА ХЕШ-ФУНКЦИЯХ

Фролов А.В., студент 565иМ гр.,
Фролов В.В., студент 565иМ гр.
Научный руководитель: доцент Певнев В.Я.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Использование квантовых компьютеров станет серьезной угрозой для нынешних стандартов информационной безопасности. Наиболее уязвимыми окажутся алгоритмы, криптостойкость которых основана на вычислительной сложности, такие как алгоритмы цифровой подписи. Использование квантовых компьютеров позволит узнать секретный ключ подписи за короткое время, что делает их не криптостойкими. Главными пост-квантовыми аналогами данных алгоритмов являются одноразовые подписи, основанные на криптостойкости хеш-функций.

Целью данной работы является исследование и сравнительный анализ существующих пост-квантовых алгоритмов цифровой подписи, основанных на хеш-функциях.

Основными пост-квантовыми алгоритмами одноразовой подписи, основанными на хеш-функциях, являются: WOTS, WOTS+ и HORS. Алгоритм WOTS является улучшением подписи Lamport, за счет использования блоков битов, а не каждого бита в отдельности. Однако данные алгоритмы сохраняют главную уязвимость подписей, основанных на хешах — зависимость от стойкости функции хеширования. Эту проблему решает алгоритм WOTS+ за счет использования масок. Общим недостатком данных алгоритмов является их одноразовость, которая частично устраняется подписью HORS. Данный алгоритм может подписывать несколько сообщений на одном ключе, при этом с каждой последующей подписью падает стойкость ключа.

Проведенный анализ показал отличия основных характеристик подписей, таких как длина ключей и подписи, а также время формирования подписи. Было показано изменение этих характеристик в зависимости от используемых параметров. На основании чего были даны рекомендации по их выбору.

УДК 004.056.55

ПОДХОД К ФОРМИРОВАНИЮ РАСПИСАНИЯ КЛЮЧЕЙ ДЛЯ БЛОЧНОГО СИММЕТРИЧНОГО КРИПТОАЛГОРИТМА ГОСТ 28147-89

Гвоздинский М. А., студент 565вМ гр.,
Научный руководитель: к.т.н., доцент Лысенко И. В.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Проблема защиты данных, в частности, обеспечения их конфиденциальности, не потеряла своей актуальности. Как правило, эта задача решается применением симметричных (блочных и поточных) алгоритмов шифрования.

Целью данной работы является описание подхода к формированию расписания ключей для блочного симметричного криптоалгоритма ГОСТ 28147-89. С этой целью в первую очередь необходимо проанализировать подходы к построению процедур формирования расписания ключей, используемых в блочных симметричных криптоалгоритмах.

Ранее уже были предприняты попытки модификации формирования расписания ключей для алгоритма ГОСТ 28147-89. Идея заключалась в объединении подходов с использованием предвычислений и непосредственного использования секретного ключа.

В общем виде идея предлагаемого решения заключается в объединении подходов с непосредственным использованием секретного ключа и преобразования ключей раундов (подключей) зависимости от преобразуемых данных.

В результате анализа было выявлено, что для реализации этого подхода требуется обеспечить однозначность использования ключей раундов в процессе шифрования и расшифрования данных. Данное условие вводит избыточность, которая является недостатком предлагаемого подхода.

Таким образом, предполагается, что подход должен повысить криптостойкость алгоритма ГОСТ 28147-89 за счёт ввода зависимости раундовых ключей от текущего значения преобразуемых данных и неизвестности для злоумышленника последовательности выбора подключей на раундах шифрования.

УДК 004.056

АНАЛИЗ ТЕХНОЛОГИИ EDELIVERY В КОНТЕКСТЕ ПРЕДОСТАВЛЕНИЯ ЭЛЕКТРОННЫХ ДОВЕРИТЕЛЬНЫХ УСЛУГ

Брошеван Е.В., студентка 565-и гр.,
Научный руководитель: профессор Потий А.В.,
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Электронные доверительные услуги согласно eIDAS включают в себя электронные подписи, штампы, метки времени, сертификаты, услуги аутентификации на веб-сайтах и регистрированную доставку документов. eIDAS также регулирует правовой статус организаций, оказывающих услуги с целью обеспечения их надежности и юридической валидности в случае возникновения споров. Чтобы Украина быть активным участником на европейском рынке необходимо организовать надлежащие условия для электронного документооборота между участниками с различными юрисдикциями. На текущий момент этому препятствуют организационные и технические обстоятельства.

В работе рассматриваются возможности внедрения электронной доверительной услуги регистрированной доставки документов с помощью технологии eDelivery, ее технические и организационные особенности, анализируется опыт внедрения в странах ЕС. Описывается процесс развертывания инфраструктуры для услуги и его проектирования, анализируются ее составные блоки: точка доступа (AP), служба метаданных (SML), служба публикации метаданных (SMP), а также протоколы взаимодействия (AS2, AS4).

Подход, используемый eDelivery, подразумевает способствование использованию существующих технических спецификаций и стандартов, а не попытки определять новые. Исходя из проанализированных особенностей можно сделать вывод, что украинская нормативная и технологическая база является достаточной для внедрения решений ЕС по eDelivery. Эта технология является универсальной и требует изучения и разработки методологии внедрения на украинском рынке электронных доверительных услуг для соответствия требованиям рынка ЕС.

УДК 004.056

АНАЛИЗ МЕТОДОЛОГИЙ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

Марченко А.О., студент 565-и гр.,
Научный руководитель: к.т.н., доцент Узун Д.Д.,
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Тест на проникновение (penetration test или pentest) – это практический способ показать, насколько защищена компания от посягательств на ее конфиденциальные данные и других угроз для информации. За рубежом также часто встречается термин этический хакинг (ethical hacking). Данный метод симулирует набор «хакерских» атак, цели которых - проникновение во внутреннюю инфраструктуру сети компании, кража и/или модификация конфиденциальных данных, нарушение работы критических бизнес процессов компании.

Такое мероприятие является необходимым для любых компаний, зависящих от информации и обслуживающих ее систем информационных технологий. К примеру, работа банковского учреждения практически полностью зависит от функционирования процессинговых систем, а интернет магазин перестанет совершать продажи в случае блокирования его веб-сайта.

Существование различных методик проведения тестов на проникновение не отменяет творческой составляющей процесса, что требует от команды, исполняющей его, глубоких познаний в сфере ИТ-безопасности и в тоже время – умения мыслить нестандартно, применять методы социальной инженерии, собирать и анализировать информацию. Существуют как открытые, так и коммерческие методологии проведения тестов на проникновение, способные при соблюдении всего процесса обеспечить гарантированное качество услуги. Использование только лишь одной методологии не является целесообразным.

По результатам анализа данных методологий была предложена авторская методика тестирования, назначением которой является оценка уровня защиты веб-приложений. Методика предназначена для стендового тестирования, однако, может использоваться для тестирования в рабочих системах.

УДК 004.056.57

ПРОГРАММНОЕ СРЕДСТВО ДЛЯ ВЫЯВЛЕНИЯ ВИРУСОВ-МАЙНЕРОВ В ЛОКАЛЬНОЙ СЕТИ

Скрябин Н.К., студент 535-і гр.,
Научный руководитель: ст. преподаватель Ильяшенко О.А.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Вследствие возросшего спроса на крипто-валюты, все чаще злоумышленниками совершаются массовые заражения компьютеров вирусами-майнерами, которые ведут «добычу» электронных денег без ведома пользователя, используя его вычислительные ресурсы, что очень сильно замедляет работу пользователя и ведет к убыткам.

Проведенный анализ показал, что на данный момент на рынке не представлены исчерпывающие программные средства (ПС) для анализа активности сетевых процессов. Существующие же решения, в силу своих архитектурных особенностей, не могут предоставить должного уровня защиты в рамках корпоративных сетей.

Объект исследования – локальная сеть. Предмет исследования – вирусы-майнеры, маскирующиеся под сетевые процессы, запущенные на компьютерах пользователей. Цель работы – обеспечение защиты локальной сети от вирусов-майнеров. К частным задачам относятся: анализ существующих ПС для обеспечения безопасности локальной сети; разработка клиент-серверного ПС. Основными функциональными требованиями, предъявляемыми к разрабатываемому ПС являются: анализ активности процессов, запущенных на компьютере клиента, формирование отчётов о подозрительной активности (название процесса, занимаемое процессорное время и т.д.), оповещение сетевого администратора посредством отправки отчетов о сетевой активности на сервер, блокировка подозрительных процессов.

В результате проведенной работы было разработано ПС, позволяющее производить анализ собранных сведений о сетевой активности, что позволяет обеспечить удаленную защиту компьютеров в рамках локальной сети вирусов-майнеров, маскирующихся под подозрительные процессы.

УДК 004.056.55

МОДЕЛЬ КРИПТОПРЕОБРАЗОВАНИЯ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ГЕНЕТИЧЕСКОГО АЛГОРИТМА НА ОСНОВЕ ПРИНЦИПА ДИВЕРСНОСТИ

Вешкин Д.А., студент 565аМ гр.,
Научный руководитель: к.т.н., доцент Лысенко И. В.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Растущая зависимость от компьютеров, как средств обработки и передачи информации между различными системами, приводит к необходимости обеспечения безопасности передаваемых данных. Так, для обеспечения конфиденциальности данных преимущественно используются симметричные криптоалгоритмы.

Целью данной работы является описание криптосистемы, основанной на принципе диверсности и использующей генетические операторы, которые, как предполагается, позволяют повысить криптостойкость алгоритма.

Ранее уже были предприняты попытки создания блочных и поточных симметричных шифров с использованием технологии генетических алгоритмов.

В общем виде идея предлагаемого подхода заключается в использовании симметричного алгоритма с сеансовым ключом, дополнительную криптостойкость которого обеспечивают генетические операторы, выбор которых в каждом сеансе взаимодействия пользователей осуществляется случайным для злоумышленника образом. Ключ шифрования и параметры алгоритма шифруются с помощью алгоритма RSA.

В результате качественного анализа напрашивается предположение, требующее проверки, что данный алгоритм имеет повышенную криптостойкость в сравнении с системами, использующими только симметричное шифрование.

Таким образом, в данной работе представлена гибридная криптосистема, основанная на принципе диверсности и использующая технологию генетических алгоритмов для повышения криптостойкости.

УДК 004.021

ИССЛЕДОВАНИЕ МЕТОДА ПОСТРОЕНИЯ ПРОСТЫХ ЧИСЕЛ

Радченко Н.В., студент 565иМ гр.,
Научный руководитель: к.т.н., доцент Певнев В.Я.,
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Задача генерации простых чисел относится к классическим вычислительным проблемам, известным с античных времен. С появлением криптографии с открытым ключом эта проблема приобрела не только теоретическое, но и большое практическое значение, так как большие случайные простые числа служат параметрами (открытыми или закрытыми) многих асимметричных криптосистем.

Двухключевые системы шифрования дали огромный импульс развития теории простых чисел. Сложность построения простых чисел обусловлена отсутствием законов распределения этих чисел. Использование псевдопростых чисел может служить основой для построения более эффективных алгоритмов для нахождения простых чисел большой размерности.

В докладе представлено теоретическое обоснование использования псевдопростых чисел для сокращения количества проверяемых чисел на простоту без пропуска простых чисел. Показана реализация построения псевдопростых чисел, которая гарантирует возможное место расположения простых чисел. Использование предлагаемого метода позволяет уменьшить количество рассматриваемых вариантов при нахождении больших простых чисел более чем в десять раз. Программная реализация метода построения простых чисел предоставит пользователю возможность генерации простых чисел и проверки их на простоту.

UDC 004.052

CONSIDERING EXPERT UNCERTAINTY DURING SAFETY ASSESSMENT OF FPGA-BASED NPP I&C SYSTEMS

Yasko A.V., Student of group 555mn,
National Aerospace University named after N.E. Zhukovsky "KhAI"

Introduction. The complexity of modern safety critical systems is becoming higher with technology level growth. Nowadays the most important and vital systems of automotive, aerospace, nuclear industries count millions of lines of software code and tens of thousands of hardware components and sensors. All of these constituents operate in integrated environment interacting with each other – this leads to enormous calculation task when the testing and safety assessment are performed.

Motivation. Traditional safety and reliability assessment methods are being constantly modified and enhanced so as to comply with increasing demands of national and international standards and guidance, as well as to be applied for I&C systems that contain number of complex components like FPGA. Although much work related to analysis of FPGA-based systems has been performed, there is a lack of detailed technique for FPGA-based I&C systems failure identification that considers probability of several faults at the same time (multi-faults), development of preventive strategies for controlling or reducing of the risk related to such failures, as well as automation of this technique so as to make it utilizable for real NPP industry tasks.

Goal. The goal of our research is to improve the quality of safety and reliability assessment by automation of assessment process and development and usage of special techniques for qualitative assessment of experts involvement.

Results. Basing on our research we propose expert involvement degree (EID) metric that indicates the level of technique automation and expert uncertainty degree (EUD) metric which is complex measure of experts' decisions uncertainty within assessment. We propose usage of total expert trustworthiness degree (ETD) indicator as function of EID and EUD.

УДК 004.056

РАЗРАБОТКА СЧИТЫВАТЕЛЯ БЕСКОНТАКТНЫХ КАРТ

Войков Ю.В., студент 535ст1 гр.,
Научный руководитель: ст. преподаватель Желтухин А.В.
Национальный аэрокосмический университет
им. Н.Е. Жуковского «ХАИ»

Считыватель бесконтактных карт, использует технологию RFID для считывания информации с карты и последующей её передачи по Wiegand, Touch Memory. Может использоваться для создания контрольно-пропускной системы или в качестве дополнительного замка для доступа к частной собственности.

Целью данного исследования является повышение безопасности эксплуатации подобных систем. Для достижения данной цели необходимо провести аналитический обзор существующих решений и решить задачу разработки действующего прототипа.

Наиболее простой и дешевый способ реализовать систему считывания бесконтактных карт – использовать плату Arduino в качестве преобразователя интерфейсов или как самостоятельную подсистему, так как её дешевизна позволяет избежать больших финансовых растрат, а обилие готовых библиотек и примеров кода сильно упрощает разработку любых систем на базе этой платформы.

Так как карты физически не защищены от возможности копирования в критически важных система необходима дополнительная проверка пользователя что бы избежать возможности несанкционированного доступа.

Простота реализации и относительная дешевизна системы позволяет при минимуме знаний и вложений получить удобную систему валидации пользователей, которая может использоваться как дома, так и на предприятии в целях повышения уровня безопасности.

УДК 004.453.3

СРЕДСТВА ПРОТОТИПИРОВАНИЯ ДЛЯ IOT СИСТЕМ ОСНОВАННЫХ НА ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ

Власов Ю.А., студент 545б гр.,
Научный руководитель: к.т.н., доцент Узун Д.Д.
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Задача развёртывания многосервисной системы на серверах, которые организованы в множество кластеров – это очень важная задача, которая во много определяет затраты времени, денежных и энергетических ресурсов, которые понадобятся для поддержки созданной системы.

Целью данного исследования является исследование средств прототипирования и контроля состояния системы, которая построена с использованием средств вирутализации. Для достижения поставленной цели необходимо решить задачу выбора системы виртуализации (к примеру, Docker, CoreOS rkt и т.п.), а также рассмотреть и подобрать систему оркестрации, которая должна следить за состоянием контейнеров и выполнять поддержку работоспособности системы в полуавтоматическом режиме.

В процессе работы, был выбран такой инструмент оркестрации множества контейнеров как Kubernetes, использование которого позволяет оптимизировать нагрузку на серверную инфраструктуру с целью максимального использования оплаченных серверов и их вычислительного времени. Такой подход позволяет уменьшить количество необходимых серверов в значительной мере, а также уменьшить трудозатраты насопровождение программного обеспечения.

Использование Kubernetes в процессе разработки и производства позволяет успешно автоматизировать большую часть процессов, которые контролируют состояние кластеров и сервисов.

Дальнейшие шаги должны быть связаны с оценкой эффективности и прибыли от использования Кубернетов в коммерческих проектах с использованием элементов теории нечеткой логики, теории графов и марковских процессов.

УДК 004.056

АНАЛИЗ ТЕХНОЛОГИИ SDN SECURITY

Годованюк П.А., студент 555м гр.,
Научный руководитель: д.т.н, профессор, Харченко В.С.
Национальный аэрокосмический университет
им. Н.Е. Жуковского «ХАИ»

Программно-конфигурируемая сеть (SDN) – это сеть для передачи данных, в которой уровень управления сетью отделён от устройств передачи данных и реализуется программно, одна из форм виртуализации вычислительных ресурсов. Современные сетевые устройства представляют собой декомпозицию из трёх составных частей: уровень управления (CLI), уровень управления трафиком и непосредственно передача трафика, под которой подразумевается физическая передачу данных на уровне микросхем и сетевых пакетов.

Целью данного исследования является повышение безопасности сетевого взаимодействия. Для достижения данной цели необходимо провести аналитический обзор существующих решений и решить задачу анализа технологии SDN Security.

В средах SDN безопасность сети SDN должна быть повсюду в сети с программным определением (SDN). Безопасность SDN должна быть встроена в архитектуру, а также предоставлена как служба для защиты доступности, целостности и конфиденциальности всех связанных ресурсов и информации.

В рамках архитектуры необходимо:
– закрепить контроллер;
– защитить контроллер;
– создать доверие;
– создать надежную политическую платформу.

В качестве направления дальнейших исследований следует выделить задачу изучения уязвимых мест и работу над их устранением. Также к приоритетному ряду задач относится повышение производительности и прохождения пакетов по минимальному пути между промежуточными узлами и устранения искажения пакетов.

АЛФАВИТНЫЙ УКАЗАТЕЛЬ

Alanamu M.A.	36
Bansi Parsania	37
Ben Hassen Jehan	32
Borbytska V.K.	24
Demidenko D.V.	38
Dube Mandlaenkosi	31
Labatt M.A.	28
Medvediev I.A.	71
Nzabahimana J.P.	25
Ouafa Dahibi	27
Parfenova I.V.	30
Peñaloza G.S.	39
Salahdine Khiarhoum	33
Tavrin A.V.	34
Yasko A.V.	99
Андриенко А.И.	58
Андрийчук А.С.	82
Белоус Н.К.	47
Бєлінський Р.А.	75
Бородавка В.В.	88
Брошеван Е.В.	94
Вешкин Д.А.	97
Власов Ю.А.	101
Войков Ю.В.	100
Гвоздинский М. А.	93
Геллер С.И.	84
Герус В.А.	43
Гладкова А.О.	53
Годованюк П.А.	102
Гулий В.В.	78
Дука И.А.	90
Землянко Г.А.	73
Зиноватный М.А.	54
Казаков Г.С.	44
Кальницкий М.Э.	69
Карпенко А.С.	85
Карпенко А.С.	86
Карпенко А.С.	87
Кийко О.Д.	91
Кирьян Е.П.	51
Косаревский Б.В.	72
Кошель М.А.	60
Кузін А.В.	50
Лаврик И.С.	42
Лаптев А.А.	45
Лаптий А.А.	46

Лукьяненко К.С.	61
Марченко А.О.	95
Москаленко Б.В.	79
Нгуен А.В.	57
Новоспасский А.С.	76
Нос Р.С.	80
Павлюков Е.А.	83
Поповиченко О.Н.	40
Почернин А.М.	81
Радченко Н.В.	98
Саєнко В.А.	68
Сверчков Д.А.	29
Сидоренко Ю.А.	48
Сидоров Я.Е.	57
Скрябин Н.К.	96
Смидович Л.Л.	26
Судаков Д.А.	65
Сушинський В.В.	64
Таланцев М.Є.	49

Тимохин И.С.	59
Тимошевський Д.С.	44
Титаренко В.С.	41
Тихонов А.В.	70
Товкало Е.П.	77
Трегуб Ю.В.	89
Третяк І.Р.	62
Третьякова Ю.Ю.	56
Федько А.Д.	35
Фролов А.В.	92
Фролов В.В.	92
Хапокныш Ю.В.	77
Хебнев А.В.	74
Хмелевцова М.А.	52
Цокота Я.В.	67
Чуйко А.А.	78
Шевяк К.И.	55
Шорский А.Э.	66
Шулінус О.А.	63

ДЛЯ ЗАМЕТОК

ПЕРСПЕКТИВНЫЕ СЕТЕВЫЕ И КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ (ПерСиК 2018)

Приведены материалы (программа и тезисы докладов) 9-й научно-технической конференции студентов «Перспективные сетевые и компьютерные технологии». Участники конференции: студенты кафедры «Компьютерных систем, сетей и кибербезопасности» Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ»; ученики лицея Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ»; студенты Харьковского радиотехнического техникума, ученики Областной специализированной школы-интернат «Одаренность», а также представители других ВУЗов Харькова.

Адрес:
61070, Украина, Харьков, ул. Чкалова, 17
Национальный аэрокосмический университет
им. Н.Е. Жуковского «ХАИ»
Аудитории:
233, 132, 123, 136в, 229 Радиокорпуса ХАИ
Время:
17 апреля 2018г., 13:30.
Рабочие языки конференции:
английский, украинский, русский
Составители:
Перепелицын А.Е., Лысенко И.В.

Перспективні мережні та комп'ютерні технології (ПерСиК 2018)

Тези доповідей НТК ПерСиК 2018

Редактори Перепелицин А. Є, Лисенко І. В.

Комп'ютерна верстка
Перепелицин А. Є.

Зв. план, 2018
Підписаний до друку 13.04.2018
Формат 60x84 1/16. Папір офс. №2. Офс. друк.
Умов. друк. арк. 7,91. Уч.-вид. л. 7,53. Наклад 100 прим.
Замовлення 3. Ціна вільна

Національний аерокосмічний університет ім. М. Є. Жуковського
"Харківський авіаційний інститут"
61070, Харків-70, вул. Чкалова, 17
http://www.khai.edu
Віддруковано ФОП Лисенко І. Б.
61070, Харків-70, вул. Чкалова, 17, моторний корпус, к. 147
Свідоцтво про внесення суб'єкта видавничої справи в державний реєстр видавців, виготовлювачів і розповсюджувачів видавничої продукції
ДК №2607 от 11.09.06 р.