

СЕКЦИЯ 4. «ТЕОРЕТИЧЕСКОЕ И СИСТЕМНОЕ ПРОГРАММИРОВАНИЕ. ЗАЩИТА ИНФОРМАЦИИ»

Гусев Ф.С. (5 к., 2 гр.), Федотов Р.С. (5 к., 2 гр.) Реализация низкоуровневых средств поддержки многооконного вывода в графическом режиме.

Научный руководитель – доц. Нестеренко В.А.

(Кафедра информатики и вычислительного эксперимента)

Представлена программная реализация доступа к графическим средствам вывода информации, доступ к графической подсистеме реализован вне рамок конкретной операционной системы.

Рыбников М.С. (4 к., 11 гр.) Компилятор простого языка с передачей параметров по имени.

Научный руководитель – доц. Савельев В.А.

(Кафедра информатики и вычислительного эксперимента)

В работе представлена реализация простого языка программирования с передачей параметров простого языка по имени.

Ермаков А.В. (4 к., 11 гр.) Защищенная система распространения XML-документов.

Научный руководитель – асс. Брагилевский В.Н.

(Кафедра информатики и вычислительного эксперимента)

В работе представлена программная архитектура и реализация системы распространения XML-документов в рамках службы WWW. Разработан протокол взаимодействия, реализованы модуль веб-сервера Apache и пользовательский агент для платформы Windows. Используется шифрование в соответствии со спецификацией XML Security.

Соловьев Л. (3 к., 11 гр.) Полное упорядочение сообщений в распределенной системе взаимодействующих эрланг-процессов.

Научный руководитель – асс. Брагилевский В.Н.

(Кафедра информатики и вычислительного эксперимента)

В работе рассматривается распределенная система взаимодействия процессов, выполняющихся на удаленных эрланг-машинах. Основная решаемая задача — упорядочение сообщений, составляющих протокол взаимодействия. Реализуется метод отметок времени (логических часов) Лампорта.

Пушенко А.В. (маг., 2 г.) Методика статического поиска скрытых групп в атрибутированных коммуникативных сетях.

Научные руководители – проф. Аграновский А.В., к.т.н. Гуфан А.Ю.

(Кафедра информатики и вычислительного эксперимента)

Представлен метод статического поиска скрытых групп в коммуникативных сетях, особенностью которого является использование атрибутов акторов сети. Кроме этого применяются метрики центральности, близости и посредничества узлов в сети. Метод является статическим и может быть применен на первом этапе динамического анализа.

Дорофеев А.А. (маг., 2 г.) Об одной модификации алгоритма RSA.

Научный руководитель – проф. Пилиди В.С.

(Кафедра информатики и вычислительного эксперимента)

Разработана модификация классического алгоритма RSA, использующая конечные расширения кольца целых чисел.

Подрезов Д.Е. (маг., 2 г.) Некоторые математические методы восстановления изображений и их сравнение.

Научный руководитель – проф. Пилиди В.С.

(Кафедра информатики и вычислительного эксперимента)

Представлены два метода восстановления изображений, содержащих области с недостающей информацией. Представлена программная реализация алгоритмов, построенных с помощью исследованных подходов. Проведен анализ скорости методов и область применимости алгоритмов.

Буртыка Ф.Б. (3 к., 11 гр.) Оптимальные алгоритмы возведения в степень

Научный руководитель – проф. Пилиди В.С.

(Кафедра информатики и вычислительного эксперимента)

Проведен сравнительный анализ некоторых алгоритмов возведения в степень.

Чекунов Е.С. (маг., 1 г.) Модель защиты от НСД на основе помехоустойчивых кодов Гоппы.

Научный руководитель — доц. Деундяк В. М.

(Кафедра алгебры и дискретной математики)

Для бинарных кодов Гоппы реализован кодек. Результаты применены для модели защиты от НСД в случаях как секретного, так и открытого ключа.

Молотников З.В. (5 к., 1 гр.) Построение параметризованного решетчатого графа. Способы его визуализации.

Научный руководитель - д.т.н., зав.каф. АДМ Штейнберг Б.Я.

(Кафедра алгебры и дискретной математики)

Разработан и реализован метод построения параметризованного решетчатого графа для фрагмента программы с внешними переменными. Найдены возможные способы его визуализации. Разработан интерфейс графического визуализатора и графический визуализатор для некоторых видов графа.

Коноплев Е.С. (4 к., 11 гр.) Использование синтаксического дерева для построения UML-диаграмм классов.

Научный руководитель — доц. Михалкович С.С.

(Кафедра алгебры и дискретной математики)

Представлена реализация построения UML-диаграммы классов по синтаксическому дереву в среде PascalABC.NET. Рассмотрен вопрос о минимально необходимой семантической информации для такого построения.

Малеванный М.С. (4 к., 11 гр.) Использование синтаксического дерева для статического анализа текста программы.

Научный руководитель — доц. Михалкович С.С.

(Кафедра алгебры и дискретной математики)

Создана библиотека запросов, позволяющих на основе синтаксического дерева программы определять ряд статических свойств кода: информацию о неинициализированных переменных, наличие косвенной рекурсии, неперехваченные исключения, характеристику параметров - переменных как выходных или входно-выходных.

Зарубин М.А. (4 к., 1 гр.) Создание препроцессора для директив компилятора PascalABC.NET.

Научный руководитель — доц. Михалкович С.С.

(Кафедра алгебры и дискретной математики)

Создан препроцессор, позволяющий обрабатывать директивы компилятора PascalABC.NET вида `{$reference 'a.dll'}`, а также директивы условной компиляции и включения файлов.

Горячий М.С. (3 к., 1 гр.) Программная реализация подсистем прозрачного шифрования и аутентификации модели защиты трафика в локальных и корпоративных сетях.

Научный руководитель — асс. Маевский А.Э.

(Кафедра алгебры и дискретной математики)

В контексте модели защиты трафика в локальных и корпоративных сетях реализованы подсистема прозрачного шифрования трафика под Unix-подобные системы и надстройка над системой аутентификации пользователей.

Баглий А.П. (5 к., 1 гр.) Автоматический контроль тестового покрытия программ при структурном тестировании.

Научный руководитель — д.т.н., зав.каф. Штейнберг Б.Я.

(Кафедра алгебры и дискретной математики)

Разработана и реализована система автоматического контроля тестового покрытия программ при структурном тестировании. Реализованы методы оптимизации такого контроля при использовании критерия покрытия передач управления в программе.

Налбандян О.В. (маг., 2 г.) Защищённая сетевая система передачи данных с электронным голосованием.

Научный руководитель — доц. Кряквин В.Д.

(Кафедра алгебры и дискретной математики)

Представлена реализация электронного голосования удалённых друг от друга участников, использующих средства сетевого взаимодействия. Приведённый протокол обработки бюллетеней обеспечивает тайность голосования и проверку его корректности при наличии центра, пользующегося доверием всех участников.

Мосин Д.А. (3 к., 1 гр.) Построение модели защиты электронного документооборота малых и средних предприятий.

Научный руководитель — асс. Маевский А.Э.

(Кафедра алгебры и дискретной математики)

Поставлена проблема защиты электронного документооборота малых и средних предприятий. Рассмотрены вопросы определения списка угроз, выбора шифров и протоколов для защиты электронного документооборота, построения политик безопасности.

Евпак С.А. (4 к., 1 гр.) Применимость некоторых классов помехоустойчивых кодов в схемах специального широкополосного шифрования.

Научный руководитель — доц. Деундяк В.М.

(Кафедра алгебры и дискретной математики)

Представлены схемы защиты тиражируемых цифровых данных, именуемые схемами специального широковещательного шифрования (ССШШ), ядром которых являются помехоустойчивые коды. Исследована применимость некоторых классов помехоустойчивых кодов в ССШШ.

Бибов А.Ю. (4 к., 1 гр.) Библиотека для вычислений в полях Галуа и помехоустойчивый RS-кодек на ее основе.

Научный руководитель — доц. Деундяк В. М.

(Кафедра алгебры и дискретной математики)

Представлена новая библиотека для вычислений в полях Галуа, позволяющая находить неприводимые многочлены заданной степени над простым полем, строить арифметические таблицы расширений простых полей, находить образующий элемент мультипликативной группы поля Галуа и т.д. Рассмотрена реализация RS-кодека на основе этой библиотеки.

Доклады призеров XXXIV научно-практической конференции ДАНЮИ

Мощенко К.О. (10 кл.) Шифрование.

Научный руководитель - Будко Л.Ф.

(МОУ СОШ №1, Сальский р-он)

На примере текстов из современных изданий, взятых из различных по жанрам источников, исследована относительная частота букв русского языка. По результатам исследования составлены четыре таблицы.