СЕКЦИЯ 4. «Теоретическое и системное программирование. Защита информации»

Бушков М.А. (маг., 2 г.) Разработка средств интеграции информационной подсистемы NSSWITCH операционной системы FreeBSD со службой каталогов LDAP

Научный руководитель – доц. **Букатов А.А.**

(Кафедра информатики и вычислительного эксперимента)

В работе приведены основные принципы использования службы каталогов LDAP. Рассматривается проблема интеграции LDAP с подсистемой NSSWITCH ОС FreeBSD. Приводится описание программных библиотек, разработанных для решения этой проблемы.

Бушманова Н. (4 к., 1 гр.) Синтаксический разбор неправильных программ

Научный руководитель – доц. **Михалкович С.С.**

(Кафедра алгебры и дискретной математики)

Построен парсер, разбирающий неправильные программы. Приведены примеры его использования для системы Intellisense среды языка программирования.

Горячий М.С. (2 к., 3 гр.) Программное средство прозрачного шифрования передаваемых по компьютерной сети данных

Научный руководитель – асс. **Маевский А.Э.**

(*Кафедра алгебры и дискретной математики*)

Представлены результаты разработки программного средства, позволяющего прозрачно для пользователя производить обработку исходящего и входящего трафика с целью его шифрования или кодирования. Средство представляет собой управляющую программу и драйвер, осуществляющий, в частности, перехват системных функций чтения/записи сокет, с возможностью масштабирования за счет добавления библиотек, реализующих различные шифры и коды.

Дорофеев А.А. (маг., 1 г.) Криптографические алгоритмы над квадратичным расширением кольца целых чисел

Научный руководитель – проф. **Пилиди В.С.**

(*Кафедра информатики и вычислительного эксперимента)*

Рассматриваются задачи, связанные с реализацией алгоритма RSA в кольце $Z[\sqrt{2}]$.

Евпак С.А. (3 к., 1 г.) Программная реализация схемы специального широковещательного шифрования.

Научный руководитель – доц. **Деундяк В.М.,** асп. **Мкртичян В.В.**

(*Кафедра алгебры и дискретной математики*)

Рассмотрена схемы специального широковещательного шифрования на основе обобщенных кодов Рида-Соломона и списочного декодера Гурусвами-Судана. Построена программная реализация этой схемы.

Ермаков А.В. (3 к., 11 гр.) Разработка крипто-модуля для веб-сервера Apache

Научный руководитель – **Брагилевский В.Н.**

(Кафедра информатики и вычислительного эксперимента)

Проведено исследование платформы веб-сервера Apache, в рамках которого изучены основные приемы реализации модулей сервера. В целях демонстрации возможностей платформы разработан модуль, поддерживающий шифрование текстовой информации перед передачей ее клиенту. В качестве конкретного приложения шифрующего модуля представлена подсистема SVN-репозитария поверх HTTP, клиентская сторона реализована средствами PascalABC.NET.

Загрядский Л.Г. (4к., 2 гр.) Практическая реализация доступа к файловой системе NTFS.

Научный руководитель – доц. **Нестеренко В.А.**

(*Кафедра информатики и вычислительного эксперимента*)

Представлена программная реализация доступа к объектам файловой системы NTFS. Доступ к файловой системе NTFS реализован вне рамок конкретной операционной системы.

Зарубин М. (3 к., 1 гр.), Коноплев Е. (3 к., 11 гр.) Реализация языка Кумир для системы программирования PascalABC.NET

Научный руководитель – доц. **Михалкович С.С.**

(Кафедра алгебры и дискретной математики)

Представлена реализация front-end компилятора школьного языка Кумир.

Иванов С. (маг., 1 г.) Реализация шаблонов типов для PascalABC.NET

Научный руководитель – доц. **Михалкович С.С.**

(Кафедра алгебры и дискретной математики)

Рассмотрены вопросы, связанные с реализацией управляемых и неуправляемых шаблонов для языка PascalABC.NET.

Кравченко Г.Ю. (4 к., 1 гр.)

Разбиение программы на кадры.

Научный руководитель – доц. Адигеев М.Г.

(Кафедра алгебры и дискретной математики)

Рассмотрен алгоритм разбиения программы на кадры. Интеграция алгоритма в Открытую Распараллеливающую Систему (ОРС).

Кравченко Е.Н. (4 к., 1 гр.)

Оптимизирующие преобразования условных операторов в распараллеливающем компиляторе ОРС.

Научный руководитель – проф. **Штейнберг Б.Я.**

(Кафедра алгебры и дискретной математики)

Представлены несколько оптимизирующих преобразований условных операторов в программе и проверки на их корректность.

Пеленицын А.М. (маг., 1 г.) О реализации декодера одного класса алгебро-геометрических кодов на проективных кривых с использованием алгоритма Сакаты

Научный руководитель – доц. **Деундяк В.М.,** асс. **Маевский А.Э.**

(*Кафедра алгебры и дискретной математики*)

Представлены результаты программной реализации алгоритма Сакаты построения множества многочленов, аннулирующих заданную двумерную рекуррентную последовательность над конечными полями. Реализация алгоритма применена для построения программного декодера одного класса алгебро-геометрических кодов.

Серова А.Г. (5 к., 1 гр.) Криптографические алгоритмы над кольцом целых гауссовых чисел

Научный руководитель – проф. **Пилиди В.С.**

(*Кафедра информатики и вычислительного эксперимента)*

Рассматривается алгоритм RSA, перенесенный на кольцо Z[i] целых гауссовых чисел. Проведены эксперименты, позволяющие судить о цикличности группы обратимых элементов фактор-кольца Z[i].

Скиба И.С. (4 к., 1 гр.) Библиотека преобразований одномерных циклов с метками в ОРС.

Научный руководитель – проф. **Штейнберг Б.Я.**

(Кафедра алгебры и дискретной математики)

Представлено несколько оптимизирующих преобразований одномерных циклов. Преобразования учитывают сохранение семантики при наличии меток и операторов перехода в теле цикла.

Хрящев М.Ю. (маг., 1 г.) Применением байесовского информационного критерия для разбиения полилога дикторов на монологические составляющие.

Научный руководитель – проф. **Аграновский А.В.**

(*Кафедра информатики и вычислительного эксперимента*)

Проведено исследование разбиения полилога дикторов на монологи. Показано применение байесовского информационного критерия для разбиения на монологические составляющие. Представлены различные способы выделения монологических составляющих. Приведены результаты исследования, показывающие возможность применения метода для решения ряда прикладных задач.

Чурилов С.А. (маг., 1 г.) Анализ безопасности и обнаружения утечек информации через протокол HTTP в корпоративных сетях

Научный руководитель – доц. **Нестеренко В.А.**

(*Кафедра информатики и вычислительного эксперимента*)

Рассмотрено понятие HTTP туннелирования. Разработана модель обнаружения утечек информации в корпоративных сетях, базирующихся на использовании HTTP туннелей и несанкционированных HTTP соединений.

Шаповалов В.Н. (маг., 1 г.), Ивченко А.В. (3 к., 1 гр.), Поважный А.В. (3 к., 1 гр.) Оптимизирующие преобразования на основе SSA формы в распараллеливающем компиляторе ОРС

Научный руководитель – проф. **Штейнберг Б.Я.**

(Кафедра алгебры и дискретной математики)

Представлены несколько преобразований программы а также графовая модель на основе SSA формы программы.

Шкутков М.М. (маг., 2 г.) Удаленное логирование в системах мгновенного обмена сообщениями

Научный руководитель – доц. **Букатов А.А.**

(Кафедра информатики и вычислительного эксперимента)

В докладе подчеркивается важность и необходимости надежного централизованного хранения логов систем мгновенного обмена сообщениями. Рассматриваются существующие решения, их достоинства и недостатки. Предлагается решение на базе мульти-протокольного клиента Pidgin.