УДК 004.43, 004.056

Г.П. Агибалов, И.А. Панкратова, Д.А. Стефанцов
Россия, Томск, Томский государственный университет

О СОБСТВЕННОМ ПРОГРАММНОМ ОБЕСПЕЧЕНИИИ УЧЕБНО-ТРЕНИРОВОЧНЫХ СРЕДСТВАХ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Сообщается о подготовке специалистов и научных исследованиях по компьютерной безопасности в Томском государственном университете на базе собственного ПО на Русском языке программирования ЛЯПАС под собственной операционной системой. Главным достоинством этого ПО является его свойство доверенности, исключающее возможность вредоносных закладок, уязвимостей и скрытых информационных каналов, присущих программному обеспечению, заимствованному у потенциального противника. Сообщается также о полигоне учебно-тренировочных средств компьютерной безопасности, на котором студенты самостоятельно, в игровой соревновательной форме, осваивают всевозможные атаки на компьютерные системы и методы защиты от них.

Доверенное программное обеспечение; компьютерная безопасность; Русский язык программирования; ЛЯПАС-Т; учебно-тренировочные средства.

Собственное программное обеспечение

Советский Союз, как известно, производил собственные ЭВМ (электронные вычислительные машины) и собственное системное и прикладное программное обеспечение (ПО) к ним. Эти ЭВМ и их ПО по своим важнейшим характеристикам и возможностям не уступали зарубежным продуктам такого рода и нередко превосходили тех, за исключением, быть может, только СуперЭВМ. В большинстве своём это были не аналоги западных образцов, но действительно результаты собственной разработки – как аппаратные, так и программные, включая микросхемы и языки программирования. Из последних наибольшую популярность среди отечественных имел специализированный язык программирования ЛЯПАС – Логический Язык для Представления Алгоритмов Синтеза дискретных управляющих систем, разработанный в Томском государственном университете (ТГУ) под руководством Аркадия Дмитриевича Закревского в начале 1960-х годов [1].

В своё время ЛЯПАС был реализован на всех отечественных ЭВМ, начиная с одноадресной машины «Урал-1» и кончая БЭСМ-10, а также на ЭВМ семейств ЕС, СМ и VAX и на персональных компьютерах первых поколений; на нём написан ряд крупных систем автоматического синтеза дискретных управляющих систем для многочисленных предприятий МЭП и МРП СССР [2–4]; его изучали, реализовывали и применяли также за рубежом – в США [5–7] как Russian Programming Language LYaPAS, в Польше [8], Югославии [9], Чехословакии, ГДР; странами – участницами СЭВ он был принят в качестве международного языка программирования. Более подробно с историей создания и развития ЛЯПАСа в советское время, с его особенностями и характеристикой систем программирования, созданных на его основе для различных типов компьютеров, можно познакомиться по обзору [10].

Применение отечественных ЭВМ и ПО, в том числе и на базе ЛЯПАСа, в системах управления критически важными объектами и технологическими

процессами способствовало обеспечению национальной безопасности страны.

Постсоветская Россия, за исключением, возможно, спецслужб, полагается повсеместно, включая и научно-образовательную сферу, на использование компьютеров и их ПО, заимствованных за рубежом, в том числе у своего же потенциального противника, вместе с содержащимися в них вредоносными закладками, уязвимостями и скрытыми каналами передачи информации [11, 12], посредством которых в страну заносится смертельная угроза для её информационной и национальной безопасности. Возрождение «русских харда и софта» стало для Отечества насущной проблемой. Свой вклад в решение этой проблемы ТГУ вносит через возрождение Русского языка программирования ЛЯПАС [13–19].

В ТГУ подготовка специалистов по компьютерной безопасности (КБ) ведётся на базе языка программирования ЛЯПАС-Т [14, 16], представляющего собой криптографическое расширение ЛЯПАСа. Принципиальное отличие этой подготовки от, судя по всему, общепринятой в России заключается в том, что она направлена в основном не на овладение существующими пакетами, системами и комплексами программ, но на разработку собственного защищённого системного и прикладного ПО, в том числе компиляторов, отладчиков, архиваторов, операционных систем (ОС), систем управления базами данных, библиотек безопасных прикладных программ, включая параллельные, реализующих алгоритмы дискретной математики, криптографии, стеганографии – с оценками их количественных характеристик в компьютерном эксперименте.

Соответственно этому, образование в области ПО КБ в ТГУ имеет три составляющие – учебную, научно-исследовательскую и внедренческую, ориентированные на освоение существующих знаний, на создание новых знаний (теоретических и практических – методов, алгоритмов и программ) и внедрение последних в учебный процесс и научные исследования.

Обучение студентов разработке собственного ПО КБ начинается с овладения ими программированием на ЛЯПАСе-Т – с представления на нём алгоритмов решения задач дискретной математики и криптографии невысокой сложности. По отзывам студентов и собственному опыту преподавания, программирование на языке ЛЯПАС на первых этапах обучения даётся намного проще, чем на языках высокого уровня, в силу того, что ЛЯПАС ориентирован именно на *представление алгоритмов* в близком к принятому в математике виде и не обременяет программиста заботами об описаниях, типах данных и др.; блок-схема алгоритма переносится на ЛЯПАС практически «один к одному». Кроме того, в это же время студенты изучают архитектуру ЭВМ, и средством для этого служит знакомство с языком ассемблера. Транслируя программы с ЛЯПАСа в ассемблер, студенты видят один и тот же алгоритм в разных представлениях (в силу простоты ЛЯПАСа, трансляция с него в ассемблер ведётся тоже почти «один к одному», в отличие от трансляции с языков высокого уровня), что помогает им лучше понять оба языка и получить представление о методах трансляции. Наиболее вдумчивые студенты при этом иногда замечают ошибки и неоптимальности транслятора, которые могут обсудить и, зачастую, исправить во взаимодействии с разработчиками последнего, которые всё время доступны и открыты для такого диалога.

Научно-исследовательская работа (НИР) студентов по созданию ПО КБ ведётся в лабораториях компьютерной безопасности и криптографии и математической криптологии и выполняется либо как часть инициативного научного проекта «Разработка доверенного ПО для создания безопасных компьютерных систем управления и связи», либо как задание на курсовые и

дипломные проекты или преддипломную практику.

Её тематика в части системного ПО включает разработку доверенных средств компиляции, распараллеливания, отладки, хранения программ на ЛЯПАСе-Т, операционной системы для подготовки и запуска программ на ЛЯПАСе-Т без участия чужих (недоверенных) ОС, тестов на безопасность (отсутствие уязвимостей и скрытых информационных каналов в) ПО на ЛЯПАСе-Т и т.п. В части прикладного ПО тематика НИР студентов ориентирована на разработку, исследование и аттестацию алгоритмов, представленных на ЛЯПАСе-Т и решающих задачи анализа и синтеза дискретных автоматов, стеганографических и криптографических систем и аппаратной реализации последних в современных программируемых средах. Исследование каждого алгоритма проводится путём опробования его на потоке случайных примеров и измерения времени и памяти, затрачиваемых компьютером на выполнение алгоритма на этих примерах. По средним, максимальным и минимальным значениям измеряемых величин, а также по результатам тестирования программы алгоритма на безопасность осуществляется аттестация его на «профпригодность».

В настоящее время ведётся создание следующих важнейших программных средств для разработки программ на ЛЯПАСе: операционной системы, транслятора, системы управления библиотеками и верификатора программ. Первые три средства реализуются на ЛЯПАСе-Т, последнее – на языке автоматизированной системы для доказательства теорем Coq.

ОС ЛЯПАС создаётся с целью получения доверенной среды создания и выполнения компьютерных программ. Важным свойством ОС ЛЯПАС является возможность выделения всех ресурсов системы единственной программе для ускорения её выполнения. Это свойство может использоваться, например, для создания и экспериментального исследования криптографических алгоритмов. На данный момент ОС ЛЯПАС запускается на компьютерах с 32-битными процессорами архитектуры x86 и поддерживает ограниченное количество устройств; взаимодействие с пользователем осуществляется на основе текстового интерфейса. В настоящий момент разработка ОС ЛЯПАС и программ для неё ведётся под управлением ОС GNU/Linux. В планах разработчика до конца 2015 года добавить возможность создания программ на ЛЯПАСе в ОС ЛЯПАС, реализовать переход на 64-битные процессоры архитектуры x86, реализовать поддержку сетевых устройств и минимальных графических возможностей для отображения букв русского и греческого алфавитов, математических символов.

Разработка транслятора с ЛЯПАСа-Т производится в три этапа. На первом этапе создаётся транслятор на C++ с ЛЯПАСа-Т в машинный код. Этот транслятор в настоящий момент используется для разработки ОС ЛЯПАС. На втором этапе он модифицируется для создания исполняемых файлов в формате ОС ЛЯПАС. На третьем этапе создаётся транслятор с ЛЯПАСа-Т, генерирующий исполняемые файлы в формате ОС ЛЯПАС, на самом ЛЯПАСе-Т. После этого транслятор третьего этапа подаётся на вход транслятору второго этапа, в результате чего получается транслятор с ЛЯПАСа-Т, работающий под управлением ОС ЛЯПАС. С этого момента разработку ОС ЛЯПАС и программ для неё можно вести в самой ОС ЛЯПАС.

Система управления библиотеками для ЛЯПАСа создаётся с целью облегчить процесс создания ПО на ЛЯПАСе-Т. Данная система создаётся по аналогии с существующими для языков Go, Rust, Ruby и Python и позволяет программистам создавать библиотеки на ЛЯПАСе-Т, загружать их на специальные серверы для последующего распространения среди других программистов,

аутентифицировать загруженные библиотеки других разработчиков с помощью цифровой подписи, вести историю усовершенствования своих библиотек с помощью механизма версий. Как показывает практика развития современных языков программирования, этот компонент является критически важным для распространения языка в среде заинтересованных программистов, готовых и желающих делиться своими наработками с единомышленниками.

Наконец, система верификации программ на ЛЯПАСе-Т [20], создаваемая на основе средства для автоматизированного доказательства теорем Coq, позволяет осуществить формальную верификацию корректности трансляции программ с ЛЯПАСа-Т в машинный код. Работа ведётся по аналогии с известным верифицирующим транслятором с подмножества C – CompCert [21], позволившим найти и исправить множество ошибок в существующих трансляторах с языка C. Дополнительно, верификаторы на Coq используются для оптимизации машинного кода при трансляции. Например, если верификатор может доказать, что одна из команд обращения к элементу комплекса (так в ЛЯПАСе называются аналоги массивов) никогда не запрашивает элемент за границами доступной памяти, транслятор может не генерировать код, осуществляющий проверку корректности индекса, тем самым ускоряя работу получаемой программы.

Результаты исследований студентов представляются на ежегодной Сибирской научной школе-семинаре с международным участием «Компьютерная безопасность и криптография» – Sibecrypt и публикуются в журнале Прикладная дискретная математика.

Аналогичным образом организована НИР аспирантов специальности 05.13.19 «Системы и методы защиты информации, информационная безопасность».

Аттестованные программные продукты, разработанные студентами и аспирантами, немедленно внедряются в учебный процесс, где они в рабочем режиме проходят тщательную отладку, и в научные исследования, где они используются в НИР последующими поколениями студентов и аспирантов.

Учебно-тренировочные средства

В отсутствие в России производственной базы, где бы студенты специальности КБ могли проходить квалифицированную практику по защите компьютерных систем, в ТГУ для этой цели функционирует полигон учебно-тренировочных средств на базе студенческой команды SiBears, трёхкратного чемпиона России и многократного участника мировых первенств в соревнованиях CTF по защите компьютерной информации. Технически полигон представляет собой локальную компьютерную сеть, подключённую к Интернет и состоящую из двух десятков компьютеров со свободным программным обеспечением под ОС Linux, размещённых в двух удалённых друг от друга компьютерных классах.

Занятия на полигоне подразделяются на теоретические, практические, игровые и состязательные. На теоретических и практических занятиях студенты самостоятельно, под руководством тренера, прошедшего в своё время через команду SiBears, осваивают различные компьютерные системы, атаки на них, методы защиты от этих атак, придумывают и проверяют в деле свои атаки и приёмы защиты от них, решают криптоаналитические задачи. На игровых занятиях студенты тренируются игре в CTF. Для этого часть из них выполняет роль жюри, а остальные разбиваются на две команды, каждая из которых устанавливает на своём компьютере полученный от жюри образ некоторой ОС с оставленными в ней скрытыми уязвимостями, настраивает его по своему разумению, пытается обнаружить «свои» уязвимости и закрыть их, и по сети пытается проникнуть в компьютер другой команды с целью захвата её флагов –

спрятанных там отрезков информации. Состязательные занятия для команды студентов выливаются в её участие в соревнованиях – в игре CTF одновременно нескольких (до сотни) различных команд, расположенных в разных уголках мира. Количество захваченных чужих и не захваченных другими её флагов служит для команды контрольной оценкой квалификации её членов в области компьютерной безопасности на текущий момент времени.

Как в теоретических, так и в практических занятиях важен регламент, который помогает участникам понять их обязанности и меру ответственности. Теоретические занятия SiBears организованы следующим образом. В начале года создаётся большой приоритезированный список тем по КБ, которые интересны в той или иной степени всем участником команды: сначала все участники методом «мозгового штурма» выбирают по несколько тем, интересных лично для них; полученные варианты объединяются в общий список; после этого начинается процедура голосования, в котором каждый участник имеет некоторое количество голосов (например, 5), которые он может распределить как угодно по полученному списку; после процедуры голосования список упорядочивается по убыванию количества полученных голосов. Каждую неделю проводится доклад на очередную тему из списка. Всякий раз докладчикам назначаются два доклада: если один из докладчиков по каким-либо причинам не сможет прийти на семинар в условленное время, его подменяет второй докладчик из пары. Срок подготовки одного доклада – месяц. Таким образом, назначение докладов происходит раз в две недели, а первые доклады начинаются через месяц после составления списка тем.

Практические занятия SiBears организованы следующим образом. Команда разбивается на три группы, каждая из которых проводит тренировку один раз в три недели и в свободное от своих тренировок время участвует в тренировках других групп в качестве игрока. Обычно еженедельная тренировка длится от 4 до 5 часов, и у играющих команд меньше участников, чем во время настоящих CTF. По этим причинам на тренировку готовится меньшее количество уязвимых сервисов, чем на настоящих соревнованиях. Как правило, это 1–2 программы. Кроме того, для новых членов команды, которым первоначально сложно включиться в процесс соревнования, готовится одно дополнительное задание, которое можно решить и тем самым повысить уровень своей подготовки.

В последнее время количество интернет-соревнований CTF, проводимых командами со всего мира, возросло, что позволяет команде в качестве тренировок участвовать в таких соревнованиях. Это даёт возможность ей готовить тренировки более тщательно, так как на учебный семестр выпадает всего 5–7 выходных, в которые не проводится какое-нибудь международное интернет-соревнование.

Вот как характеризует основные образовательные достоинства игры в CTF один из действующих членов команды SiBears – Георгий Зайцев.

«Один из главных навыков, которые получают студенты, играющие в CTF, – это умение искать и вычленять полезную информацию. В век информационных технологий оно является важнейшим в жизни человека. Зачастую, на соревнованиях CTF приходится сталкиваться с новыми технологиями и, не имея опыта работы с ними, крайне важно в кратчайшее время разыскать необходимые знания. При этом нужно не просто научиться «включать, чтобы работало», но и правильно настроить, чтобы обеспечить защиту от атак соперника. Ввиду того, что разные соревнования организуются разными людьми, каждое конкретное соревнование состоит из решения задач, которые конкретные организаторы считают интересными. Например, на одних соревнованиях криптографические задания могут касаться только эллиптических кривых, поскольку автор заданий

занимается их исследованием, а на других соревнованиях участникам приходится иметь дело с конечно-автоматными криптосистемами – с любимым предметом другого организатора. Так по воле разных организаторов соревнований их участники вынуждены обретать разные новые знания. Поэтому знания, полученные членами команды SiBears, нередко выходят за рамки учебной программы ТГУ и зачастую имеют практически направленный характер, недостижимый в пределах этой программы.

Кроме того, решая на соревнованиях задачи, максимально приближенные к потребностям работодателей, студенты могут определить, насколько им близка та или иная сфера деятельности. Выбрав направление, человек сам начинает искать необходимую информацию и тем определяет качество своего обучения самостоятельно (без участия преподавателя). Данный подход лишён главного недостатка, который возникает при традиционном методе обучения (преподавателем) – потери интереса к предмету, так как студент сам выбирает интересующую его область и осознанно тратит свободное время на её изучение. С другой стороны, отсутствие преподавателя, который может помочь, указав направление, куда стоит двигаться, зачастую ставит новых людей в тупик, поскольку осознание того, что лучший способ научиться что-то делать – это найти необходимую информацию самостоятельно, приходит не сразу. В частности, по этой причине не все студенты, приходящие в команду на первом курсе, удерживаются в ней и на следующих курсах».

Студенты, прошедшие в полной мере обучение и тренировки на полигоне, получают, как правило, отличные оценки и на государственном экзамене, и за защиту дипломных работ. Задолго до окончания университета они расхватываются работодателями и в компьютерной безопасности скоро становятся специалистами мирового уровня. Не случайно кафедра защиты информации и криптографии, осуществляющая их подготовку в ТГУ, в 2014 году стала Образовательным центром года РФ в области информационной безопасности, а её студент Брославский Олег – Студентом года.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Закревский А.Д.* Алгоритмический язык ЛЯПАС и автоматизация синтеза дискретных автоматов. Томск: Изд-во Том. ун-та, 1966. 266 с.

2. Синтез асинхронных автоматов на ЭВМ / Под ред. А.Д. Закревского. Минск: Наука и техника, 1975. 184 с.

3. Автоматизация проектирования цифровых устройств / Под ред. С.С. Бадулина. М.: Радио и связь, 1981. 238 с.

4. *Панкратова И.А., Быкова С.В., Николаева Л.А., Оранов А.М.* Система автоматического синтеза комбинационных схем СИНТЕЗ-Ф // Управляющие системы и машины. 1991. № 1. С. 3–9.

5. LYaPAS: A programming language for logic and coding algorithms / Ed. by M.A. Gavrilov and A.D. Zakrevskii. New York and London: Academic Press, 1969. 475 p.

6. *Charles J., Albright Jr.* An interpreter for the language LYaPAS. University of North Carolina at Chapel Hill: Department of Computer Science, 1974. 127 p.

7. *Nadler N.* User group for Russian programming language // IEEE. Newsletter for Computer-Aided Design. Iss. 3. May/June, 1971.

8. *Michalski A., Wiewiorowski T.* Odra Ljapas. Warszawa: Computation-Centre Polish Academy of Sciences, 1970. 33 p.

9. *Tratnik I.* Seminar «Analiza in primer java jezikov zapodro'jedigitalnetehnike». Lljubljani: Univerzav, 1979. 63 с.

10. *Торопов Н.Р.* Язык программирования ЛЯПАС // Прикладная дискретная математика. 2009. № 2(4). С. 9–25.

11. *Колегов Д.Н., Брославский О.В., Олексов Н.Е.* Об информационных потоках по

времени, основанных на заголовках кэширования в протоколах HTTP // Прикладная дискретная математика. Приложение. 2014. № 7. С. 89–92.

12. *Милованов Т.И.* О скрытых каналах по времени в ОС Android // Прикладная дискретная математика. Приложение. 2014. № 7. С. 92–94.

13. *Агибалов Г.П.* К возрождению Русского языка программирования // Прикладная дискретная математика. 2012. № 3(17). С. 77–84.

14. *Agibalov G.P., Lipsky V.B., Pankratova I.A.* Crypto graphic extension of Russian programming language // Прикладная дискретная математика. Приложение. 2013. № 6. С. 93–98.

15. *Agibalov G.P., Lipsky V.B., Pankratova I.A.* Project of hardware implementation of Russian programming language // Прикладная дискретная математика. Приложение. 2013. № 6. С. 98–102.

16. *Агибалов Г.П., Липский В.Б., Панкратова И.А.* О криптографическом расширении и его реализации для Русского языка программирования // Прикладная дискретная математика. 2013. № 3 (21). С. 93–104.

17. *Agibalov G.P., Lipsky V.B., Pankratova I.A.* About cryptographic extension of Russian programming language and its soft and hard implementations // International Congress on Computer Science: Information Systems and Technologies. Proceedings. Republicof Belarus. Minsk, November' 4–7, 2013. P. 127–132.

18. *Агибалов Г.П.*О работах по созданию доверенного программно-аппаратного обеспечения для синтеза безопасных компьютерных систем логического управления на базе Русского языка программирования // Решетнёвские чтения: материалы XVII Международной научн. конф., посвящ. памяти генер. конструктора ракет.-космич. систем акад. М.Ф. Решетнёва (12–14 нояб. 2013 г., Красноярск), в 2 ч. / Под общ. ред. Ю.Ю. Логинова: Сиб. гос. аэрокосмич. ун-т. Красноярск, 2013. Ч. 2. С. 275–277.

19. *Грибанов А.С., Сибирякова В.А.* Программная реализация операций над большими числами в языке ЛЯПАС-Т // Прикладная дискретная математика. Приложение. 2014. № 7. С. 146–148.

20. *Жуковская А.О., Стефанцов Д.А.* Разработка автоматизированного средства для доказательства свойств программ // Прикладная дискретная математика. Приложение. 2014. № 7. С. 148–150.

21. compcert [Электронный ресурс]. http://compcert.inria.fr/

УДК 004.056

А.С. Андреев, А.М. Иванцов
Российская Федерация, Ульяновск, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Ульяновский государственный университет»

ОПЫТ ПРИМЕНЕНИЯ КОМПЛЕКСОВ (ПОЛИГОНОВ) В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Статья посвящена опыту применения комплексов (полигонов) градообразующих предприятий Ульяновска в процессе обучения студентов, обучающихся по специальности «Компьютерная безопасность». Для доступа студентов к современным комплексам (полигонам) в процессе обучения на факультете университета были созданы базовые кафедры при предприятиях, которые обеспечивают возможность практической работы студентов на современном оборудовании предприятий.

Опыт применения комплексов (полигонов); обеспечение информационной безопасности; производственные и преддипломные практики; базовые кафедры при градообразующих предприятиях.