УДК 004

**Г.П. Агибалов, И.А. Панкратова**

Россия, Томск, Томский государственный университет

# НАУКА НА СЛУЖБЕ ОБРАЗОВАНИЮ В ОБЛАСТИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Сообщается о роли и месте науки в подготовке специалистов по компьютерной безопасности в Томском государственном университете в условиях ограниченной потребности в них со стороны отечественных работодателей и неограниченной потребности в них со стороны работодателей в Западной Европе и Соединённых Штатах Америки.

Ключевые слова: компьютерная безопасность; подготовка специалистов; научные исследования.

В отсутствие в стране состоятельных работодателей, заинтересованных в специалистах по компьютерной безопасности (КБ) и способных составить конкуренцию работодателям из Западной Европы и Соединённых Штатов Америки в материальном обеспечении таких специалистов, их подготовка с ориентацией на отечественных потребителей стала не только нецелесообразной и бессмысленной, но и в значительной степени вредоносной для страны. Это становится совершенно очевидным, если учесть «пограничный» характер специалистов в области КБ и тот факт, что ¾ выпускников отдельных вузов России, в том числе и ТГУ, получивших образование в этой области, работают не в России, но как раз на «дружественном» Западе, куда их принимают без лишней суеты – по одному названию выпустившего их университета, указанному ими в резюме. Кроме того, в Советском Союзе однажды уже проводилась подготовка специалистов, ориентированная на работодателей, – так называемая Целевая Интенсивная Подготовка Специалистов (ЦИПС) в интересах предприятий конкретных министерств (в ТГУ – электронной и радиопромышленности), которая разделила судьбу СССР и прекратила своё существование вместе с соответствующими министерствами, вернув университеты к прежней системе образования, направленной на овладение студентами не умений, потребных для работодателя, но новых знаний, потребных для человечества, включая работодателей, и создаваемых на базе научных исследований. Наступать дважды на одни и те же грабли в данном случае не только не-

прилично. Наконец, любое образование, будь оно в интересах работодателей или нет, невозможно без опоры на науку.

Основным мотивом образования по КБ на базе науки должна служить постоянно возрастающая потребность Родины в специалистах, способных обеспечить ей информационную безопасность в условиях повсеместного распространения всё более «умных» компьютерных атак. Эффективное противодействие этим атакам возможно лишь на основе отечественного программно-аппаратного обеспечения компьютерных систем, криптографических методов защиты информации в них на базе результатов фундаментальных научных исследований и патриотически воспитанных специалистов. Именно этот тезис является основным в организации в ТГУ образовательной программы по КБ на кафедре защиты информации и криптографии (ЗИК).

Учебно-производственный план специальности КБ в ТГУ предусматривает выполнение студентом курсовых и дипломной работ и прохождение двух видов практики – учебной и предквалификационной (преддипломной) – под руководством преподавателя кафедры, сотрудника отдела КБ Управления информатизации (УИ) ТГУ или выпускника кафедры, работающего в Томском отделении **ЗАО «Позитив Текнолоджис»**. Все эти работы студента – курсовые, дипломная и практические – являются научно-исследовательскими. Научный руководитель студента формулирует ему тему для самостоятельного исследования и контролирует его работу над ней. Темы формулируются по актуальным научным проблемам специализаций «Математические методы защиты информации» и «Анализ безопасности компьютерных систем» и касаются, главным образом, моделей безопасности компьютерных систем, 11нновационноческих и стеганографических методов защиты информации в них, угроз безопасности криптографических и компьютерных систем и атак на них.

Целью курсовых работ и учебной практики является приобщение студентов к научно-исследовательской работе по специализациям кафедры. Цель предквалификационной практики – создать необходимый задел для последующего успешного выполнения квалификационной (дипломной) работы, которая в ТГУ, в соответствии с квалификацией специалиста, носит характер математического исследования с присущими ему атрибутами – определениями, теоремами, доказательствами, математическими моделями, методами, алгоритмами, программами, оценками и т.п. Она может быть теоретической – с результатами в форме теорем, моделей и методов и (или) практической – с комплексом алгоритмов и программ в качестве основного результата. Исследовательский аспект практической работы выражается в построении оценок

эффективности созданных алгоритмов и программ и (или) параметров моделируемых ими объектов. Эти оценки могут быть аналитическими и (или) экспериментальными. Последние получаются путём компьютерного моделирования алгоритмов на множестве всех, случайных или специальным образом подобранных, тестовых примеров. Темы квалификационных работ ставятся, как правило, в развитие исследований, выполненных студентами на предквалификационной практике, и выполняются также, как правило, по месту прохождения последней и под прежним руководством.

Наиболее успешные студенты привлекаются к работе на кафедре для выполнения научных грантов РФФИ, принимаются на должности программистов в отделе КБ УИ ТГУ или **ЗАО «Позитив Текнолоджис» для** выполнения научных исследований по их тематике, что позволяет студентам получать дополнительные научные и практические знания и навыки в области КБ.

Ежегодно, начиная с 2002 г., кафедра ЗИК проводит Всероссийскую конференцию «Сибирская научная школа-семинар «Компьютерная безопасность и криптография» – SibeCrypt» с участием учёных, аспирантов и студентов из России и стран ближнего и дальнего зарубежья. На ней до 10 докладов делаются студентами кафедры ЗИК. См. сайт http://sibecrypt.tsu.ru.

С 2008 г. кафедра издаёт научный журнал «Прикладная дискретная 12нтематика» – ПДМ, входящий в Перечень ВАК и в международные базы цитирования Scopus и MathSciNet. В нём публикуются статьи отечественных и зарубежных авторов по всем важнейшим разделам дискретной математики и её приложениям, в том числе в компьютерной безопасности и криптографии, он рекомендован УМО Минобрнауки в области информационной безопасности вузам страны для использования в научных исследованиях и учебном 12нновацсе в этой области. В нём регулярно публикуют свои научные работы и студенты кафедры ЗИК, проходя рецензирование на равных с маститыми учёными. См. сайты http://vestnik.tsu.ru/pdm или http://mathnet.ru/.

На базе кафедры ЗИК создана и получает подготовку студенческая команда SiBears, участвующая регулярно в международных соревнованиях CTF (Capture The Flag) по защите компьютерной информации и регулярно занимающая в них призовые места среди многих десятков команд университетов мира. Она – трёхкратный чемпион России, входит в десятку лучших профессиональных команд в мире. Подготовка в команде служит дополнительной не только учебной лабораторией, в которой студенты специальности КБ овладевают практическими навыками защиты компьютерных систем от взлома злоумышленниками, но и дополнительной научной лабораторией, где они разра-

батывают методы обеспечения стойкости процесса соревнования CTF к атакам со стороны нечестных участников. См. сайт http://sibears.ru/

При кафедре ЗИК функционирует бесплатная школа юного «криптографа-безопасника», в которой под руководством студентов-старшекурсников десятки учащихся 8-11-х классов школ Томска знакомятся с элементами 13нтематических основ криптографической защиты информации и компьютерной безопасности и решают простейшие задачи анализа защищённости и создания средств защиты компьютерных систем от возможных атак. Обучение школьников в ней ведётся с целью их профориентации, проявления в них интереса к научной работе по обеспечению безопасности компьютерных систем и подготовки их к участию в российских олимпиадах по математике и криптографии для поступления в ТГУ на специальность КБ. И надо сказать, что работа школы приносит неплохие плоды: средний балл абитуриентов, поступающих на кафедру, превосходит 250.

Учебный процесс и прикладные научные исследования в области компьютерной безопасности и криптографии кафедра осуществляет на основе свободного и проприетарного ПО на собственном языке программирования ЛЯПАС-Т, разработанном специально для представления алгоритмов дискретной математики, решающих задачи криптографической защиты информации, и тем самым развивает в студентах умение разрабатывать, исследовать и развивать собственные защищенные программные продукты и избавляет их от необходимости использования недоверенного и неконтролируемого ими лицензионного программного обеспечения, к тому же ещё и дорогостоящего, а самое главное – не безопасного. В обучении студентов участвуют 10 профессоров-докторов наук и более 20 доцентов-кандидатов наук. Теоретическое содержание большинства дисциплин профессионального и специального циклов ООП основывается на результатах научных исследований преподавателей этих дисциплин. Разработчиками же системного и прикладного обеспечения на ЛЯПАСе-Т, используемого в обучении, включая компилятор и ОС, являются сами студенты.

Вот некоторые достижения студентов кафедры за последние 3 года:

1) исследование свойств дифференцируемых функций в конечных полях и кольцах, опубликовано в журнале Groups, Complexity, Cryptology (А. Ивачёв); прототип защищенной СУБД MySQL и прокси-сервер СУБД (Database Firewall) с мандатным управлением доступом (Н. Ткаченко); обнаружение и описание новых скрытых каналов передачи информации в протоколе HTTP и ОС Android (О. Брославский, Н. Олексов, Т. Милованов); защищённая про-

граммная платформа BlackBox для проведения соревнований CTF (Н. Анисеня, Т. Торгаева, Г. Зайцев); прототип защищенной облачной СУБД с сохранением порядка (И. Глотов, С. Овсянников); обнаружение уязвимостей и ошибок безопасности в сервисах крупнейших Интернет-компаний MailRu, Yandex, Twitter, Badoo, Olark, Foursquare, SoundCloud, iFixit и др. с благодарностями компаний за ответственные сообщения о них;

2) доклады на международных конференциях: по ИБ – «Positive Hack Days» и «Zero Nights» (Москва, 2014 – 2016), «Zero Nights» (Москва, 2014), «F5 International Product Development Summit» (Тель-Авив, 2014), по математике – Мальцевские чтения (Новосибирск, 2014), Алгебра и математическая логика (Казань, 2014); на Всероссийской конференции SibeCrypt (Иркутск, 2012; Томск-Парабель, 2013; Екатеринбург, 2014; Новосибирск, 2015, 2016);

3) призовые места на конкурсах лучших научных работ по ИБ на форуме «Positive Hack Days» (2013 – 2014), победы в номинации «Студент года» Всероссийского конкурса «Инфофорум» (О. Брославский, 2015; А. Ивачев, 2016).

Учебный процесс и научные исследования на кафедре ЗИК постоянно поддерживаются грантами РФФИ (на школу-семинар SibeCrypt и на научный проект «Криптосистемы с функциональными ключами»), ТГУ (по Программе повышения конкурентоспособности) и ФЦП «Кадры» (на научно-исследовательские проекты и международную конференцию с элементами научной школы для молодёжи по компьютерной безопасности и криптографии).

Для выпускников специальности КБ в ТГУ есть аспирантура и совет по защите кандидатских и докторских диссертаций по специальности 05.13.19 «Методы и системы защиты информации. Информационная безопасность» (физико-математические и технические науки). За последние 10 лет на кафедре защищены 1 докторская и 7 кандидатских диссертаций.

Всё перечисленное – и фундаментальные научные исследования в дискретной математике, и приложения их результатов к компьютерной безопасности и криптографии, и учебно-методическая работа на их основе, и создание свободного ПО на базе собственного языка программирования ЛЯПАС, и большая подготовительная работа со школьниками – всё это делает наших выпускников особенно успешными в исследовании и разработке собственных систем защиты информации, обеспечивающих более высокий уровень безопасности и являющихся абсолютно доверенными, чего не скажешь про импортные средства защиты. В условиях жёсткой конкуренции эти свойства систем ИБ, обеспечиваемые выпускниками ТГУ, гарантируют последним высокую востребованность квалифицированными работодателями.