тестировании: организация режима обучения: возможность проведения тестирования в сетевом, локальном варианте и т. д.).

3. *Требования к отчетности* (формирование файлов краткого и полного отчетов; защита результирующего файла от несанкционированного доступа на чтение и редактирование; возможность централизованного сбора результатов тестирования и т. д.).

4. *Требования к тестовой оболочке* (удобство интерфейса; наличие в системе гибкой системы настроек режимов проведения теста, выбор критериев оценок и т. п.; возможность организации применения подготовленного теста как для контроля, так и для самоконтроля знаний и т. д.).

По каждой номинации программы оцениваются отдельно. О профессионализме студентов как разработчиках говорит тот факт, что в настоящее время некоторые программы, участвующие в конкурсе и имеющие научную направленность, используются различными лабораториями ИМФИ в реальных исследованиях. Ряд программ получили регистрационное свидетельство Федерального депозитария электронных изданий (НТЦ «Информрегистра»). Работа по созданию и использованию программных продуктов продолжается.

Развитию профессионализма, а также активизации познавательной деятельности студентов способствует их участие в различных олимпиадах и чемпионатах. Впервые на базе кафедры информатики и информационных технологий ИМФИ Тамбовского государственного университета им. Г.Р. Державина в 2006 г. проводился чемпионат по командному программированию. В чемпионате приняло участие 28 команд, всего 76 участников, среди них студенты 1–5-х курсов всех специальностей ИМФИ, ученики ТОФМЛ, студенты ТГТУ.

Чемпионат проводился по следующим правилам: 1) готовое решение не должно взаимодействовать с пользователем. В качестве решения задачи рассматривается только выходной файл, полученный в пределах допустимого времени; 2) за каждую попытку подачи решения, начиная со второй, вычитаются штрафные баллы (как правило, 2 % от максимального балла за задачу); 3) если специально не указаны ограничения, то считается, что программа должна представить решение через 2 с. Время засекается по КС жюри; 4) содержимое всех файлов представлено в кодировке windows-1251; 5) строки в текстовом файле разделяют два подряд идущих символа с ASCII-кодами 13 и 10 соответственно (т. н. символы новой строки CR/LF); 6) пробельным символом считается любое число подряд идущих символов пробелов, табуляции и новой строки; 7) все задачи имеют корректные входные данные; 8) подразумевается, что каждый пример имеет единственный ответ; 9) количество тестов и их конкретное содержание жюри не разглашается.

Для испытаний участникам было предложено 5 авторских задач различной сложности (максимальный балл оценки решения задачи от 20 до 300). Для решения всех задач требовались знания в рамках стандартных университетских курсов по алгоритмическому программированию. После решения каждой задачи участники предоставляли судье файл с решением, которое проверялось жюри. Проверка решений производилась в полуавтоматическом режиме с помощью специального программного обеспечения на тестах, предоставленных авторами задач. По окончании проверки решения жюри сообщало результаты проверки: решена ли задача полностью, сколько набрано баллов с учетом штрафов, таблицу результатов всех команд.

Из 28 команд решение одной и более задач предоставили 18 команд. По результатам проведения Чемпионата ИМФИ по командному программированию были определены три команды-победители, которым были вручены соответствующие дипломы. Команды-призеры были рекомендованы к участию в ¼ Чемпионата мира по командному программированию в 2006 г.

На основе интереса к Чемпионату со стороны студентов и пожеланий участников предполагается проведение Чемпионата ИМФИ по командному программированию каждый учебный семестр.

Поступила в редакцию 16 октября 2006 г.

ПОЛИТИКА БЕЗОПАСНОСТИ МНОГОПОЛЬЗОВАТЕЛЬСКИХ КОМПЬЮТЕРНЫХ СИСТЕМ, ИСПОЛЬЗУЕМЫХ В ОБУЧЕНИИ

© Д.В. Лопатин, Е.С. Чиркин

Lopatin D.V., Chirkin E.S. The policy of security of the multiuser computer systems used in training. The decisions for the policy of security of workstations for the multiuser systems are developed.

Проблема стабильной работы компьютерных классов университета стоит весьма остро. Это связано с многопользовательским режимом использования компьютерных систем, большим числом читаемых курсов и специальностей. На кафедре информатики и информационных технологий ТГУ им. Г.Р. Державина разработаны решения для построения системы, основанной на политике информационной безопасности рабочих станций.

Система строится на использовании файловой системы NTFS как единственной файловой системы, отвечающей предъявляемым требованиям политики безопасности и аудита. Использование доменной архитектуры сети, для чего выделен отдельный постоянно

доступный сервер – контроллер домена с ActiveDirectory под управлением Windows 2003 Server, упрощает централизованное управление и повышает удобство использования политики безопасности.

В системе допустимо пять типов учетных записей (аккаунтов): администраторы, которые отвечают за нормальное функционирование программной и аппаратной части домена, студенты, преподаватели, резервные и «гостевые» пользователи. Пароли ко всем типам аккаунтов назначаются администратором. Все учетные записи, кроме резервных и «гостевых», являются именными. Подразумевается, что пользователь несет полную ответственность за действия, совершенные под его аккаунтом. Резервные учетные записи предназначены для использования в форс-мажорных обстоятельствах, когда невозможен обычный вход в домен. Аккаунты типа «гостевые» предназначены для школьников и учащихся заочного отделения, они имеют существенные ограничения и доступны для входа только в отведенные для этого часы. Учетные записи типа «преподаватель» по сравнению с типом «студент» имеют увеличенные квоты на использование дискового пространства и разрешена запись в некоторые специальные ресурсы на сервере, доступные остальным только для чтения. Для всех типов записей ведется аудит действий для разрешения спорных случаев и обнаружения несанкционированных действий.

Приведем наиболее важные определения политики безопасности.

Профиль – множество пользовательских настроек (темы оформления, звуковые схемы, обои рабочего стола и т.п.), ветвь HKEY_CURRENT_USER реестра Windows, папка «Мои документы», «Избранное» и др. По умолчанию профиль находится в папке c:\Documents and Settings\<user> (часть папок может быть вынесена оттуда путем специальных настроек). Локальный профиль – это профиль пользователя, находящийся на том же компьютере, на котором пользователь вошел в систему. Перемещаемый профиль – профиль пользователя, хранящийся на специальном сервере. Каждый раз, когда пользователь регистрируется в системе, создается локальная копия перемещаемого профиля, с которой впоследствии и работает пользователь. При выходе пользователя из системы все изменения, сделанные в локальном профиле, сохраняются на сервере, т. е. профиль как бы «перемещается» вслед за пользователем, на каком бы компьютере локальной сети он не зарегистрировался (ограничение: один и тот же пользователь может быть одновременно зарегистрирован только на одном компьютере локальной сети).

Ограничение использования свободной дисковой памяти – с целью рационального использования свободной дисковой памяти сервера вводится ограничение на суммарный размер файлов и профиля, которые могут находиться на сервере у каждого конкретного пользователя – 30 Мб. Следует учесть, что часть этого пространства резервируется операционной системой под свои нужды и не доступна пользователю.

Файлы и папки. Все пользовательские файлы на сервере проверяются антивирусом, у которого действие по умолчанию для детектированных вредоносных программ – удаление. Для каталога "c:\temp" – запись и чтение разрешены всем, сохранность содержимого после перезагрузки, входа или выхода пользователя или по наступлении иных событий (например, вследствие противоречия содержимого папки политике безопасности) не предусматривается. Для каталога "c:\stud" – запись и чтение разрешены всем, содержимое удаляется автоматически по необходимости (например, в связи с нехваткой свободного места или согласно политикам безопасности и т. п.). Файлы с расширениями .tmp или .$$$ или без расширения считаются временными и удаляются автоматически по мере необходимости. Файлы, которые могут быть классифицированы, – «автоматические резервные копии», удаляются, если их возраст превышает 15 дней. Аналогично, некоторые папки и файлы профиля, не влияющие на функционирование системы, могут удаляться автоматически. Пользователям рекомендуется своевременно удалять ненужную информацию, в том числе это позволит сократить времена входа и выхода из системы.

Ограничения политики безопасности. Запрещается производить действия, мешающие нормальному функционированию локальной сети, а также изменять IP-адрес компьютера. Запрещается устанавливать обои рабочего стола, фоновые рисунки папок, а также производить любые другие настройки, противоречащие нормам общепринятой морали. Запрещается препятствовать работе установленных антивирусных средств.

В случае обнаружения какого-либо противоречия политикам безопасности исправления могут вноситься автоматически или администраторами без предупреждения. В случае вины пользователя к нему могут быть приняты меры административного воздействия.

Поступила в редакцию 16 октября 2006 г.