Г. П. Аверьянов, В. А. Будкин, В. В. Дмитриева, А. М. Коршунов, А. А. Фадеев

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕВОГО УЧЕБНО-НАУЧНОГО ЦЕНТРА ПО ЭЛЕКТРОФИЗИКЕ

Введение

При разработке учебно-научного информационно-вычислительного центра на кафедре электрофизических установок МИФИ важнейшее значение имеет обеспечение сохранности и целостности быстро изменяющихся информационных ресурсов центра. Актуальность защиты информации сейчас не отрицает никто. Однако основные задачи этой области и последствия пренебрежения ими могут быть совершенно различными. В связи с этим структура программно-аппаратных средств в значительной степени зависит от требований, предъявляемых конкретными приложениями.

Если вопросы защиты информационных систем органов государственной власти, промышленных предприятий, учреждений кредитно-финансовой сферы, банков и т. п. достаточно очевидны и хорошо проработаны, то особенности информационных систем компьютерных учебных центров и необходимость защиты их информационных ресурсов от действия случайных и преднамеренных факторов не столь очевидны и в каждом конкретном случае нуждаются в тщательной проработке, особенно в связи с развитием так называемого дистанционного обучения.

На протяжении более чем тридцати лет на кафедре электрофизических установок проводятся работы по введению в практику проведения учебных занятий различных форм компьютерных информационных технологий. Последний этап этих работ связан с созданием центрального кафедрального информационно-вычислительного центра для поддержки учебных циклов: ускорители заряженных частиц (УЗЧ), вакуумная техника, техника СВЧ, физическая электроника, СВЧ-энергетика, электронные системы УЗЧ, информационные системы УЗЧ (ИСУ). Наряду с традиционными видами деятельности студентов, такими как учебно-исследовательская работа (УИР), курсовое проектирование (КП), дипломное проектирование (ДП), требующими как информационных, так и вычислительных ресурсов, особое место занимают компьютерные лабораторные практикумы (как правило, для студентов младших курсов), которые разработаны практически во всех перечисленных циклах и могут выполняться как в кафедральном, так и в институтских компьютерных классах. Это наиболее массовый вид занятий с применением сетевых информационных технологий. Для всех видов занятий на центральном сервере хранятся постоянно обновляемые как индивидуальные, так и групповые архивы студентов, в которых

сохраняется выполняемая ими работа, а также размещаются различные методические указания, индивидуальные задания, учебные пособия и наиболее важная научная литература.

В связи с этим загрузка центрального сервера оказывается значительной. Так, например, в одном из наиболее насыщенных лабораторными практикумами циклах ИСУ проводятся занятия в компьютерных классах для двадцати групп студентов дневного факультета и примерно такого же количества групп вечернего факультета. Практически это означает необходимость поддерживать сохранность около 900 личных архивов, которые находятся в постоянном интерактивном воздействии и изменении. При этом периодичность смены владельцев архивов и обновление в них информации различны и зависят от вида занятий (для ДП не менее года, а в лабораторных практикумах могут меняться в течение семестра). И хотя информация в студенческой базе данных, включающая выполняемую ими работу в рамках учебного плана, разумеется, не представляет государственной тайны и не связана с кредитно-денежными операциями, ее нарушение или потеря, а также несанкционированный доступ (что часто случается) могут значительно осложнить проведение учебного процесса. При этом необходимо учесть, что права доступа разных студентов к разным видам информационных ресурсов должны быть различными. Это, прежде всего, кафедральный компьютерный класс, в рамках которого находится основной сервер учебно-научного центра электрофизики (основной информационный ресурс), все средства, включенные в сеть кампуса МИФИ, — институтские учебные компьютерные классы, ПК учебно-научных лабораторий кафедры. Возможен также доступ с домашних компьютеров студентов и преподавателей, которым предоставлены соответствующие права доступа. Таким образом, студентам предоставляется в режиме удаленного доступа возможность дополнительной самостоятельной удаленной работы в рамках разнообразных форм учебных занятий, а преподавателям — возможность выполнения методической работы. Одна из главных задач разработки связана с обеспечением надежной работы основного информационного ресурса — центрального сервера ЛВС компьютерного класса кафедры, который включает большое количество личных архивов студентов, методические материалы, различное инструментальное и прикладное программное обеспечение.

Это требует разработки комплекса мер защиты информации как от случайных (непреднамеренных), так и от преднамеренных внешних воздействий и нежелательных внутренних взаимодействий пользователей (студентов) в рамках рабочей среды.

Все это предполагает жесткое администрирование и своевременное выполнение профилактических работ в системе.

1. Общесистемное аппаратно-программное обеспечение центра

На рис. 1 представлена схема кафедрального учебно-научного центра со всеми необходимыми внешними связями и аппаратным обеспечением информационной безопасности.

Сеть состоит из основного сервера, компьютерного класса с рабочими станциями, сетевого коммутатора и шлюза в сеть Интернет. В качестве рабочих ОС применяются Windows XP и Debian GNU/Linux. ОС семейства Windows используются очень широко, поэтому ее поддержка была необходима. ОС Debian GNU/Linux была выбрана как постепенная замена Windows XP. Debian GNU/Linux содержит в своей поставке огромное (более 10000) число программ самой широкой направленности, нетребовательна к ресурсам ПК, не требует приобретения лицензий для использования, имеет длительную поддержку обновлений безопасности, хорошую документацию и поддержку со стороны разработчиков и других пользователей. Кроме этого, программа установки Debian GNU/Linux позволяет производить установку и обновление этой ОС с самых различных носителей полностью в автоматическом режиме (режим preseed). Это особенно удобно при обслуживании компьютерного класса.

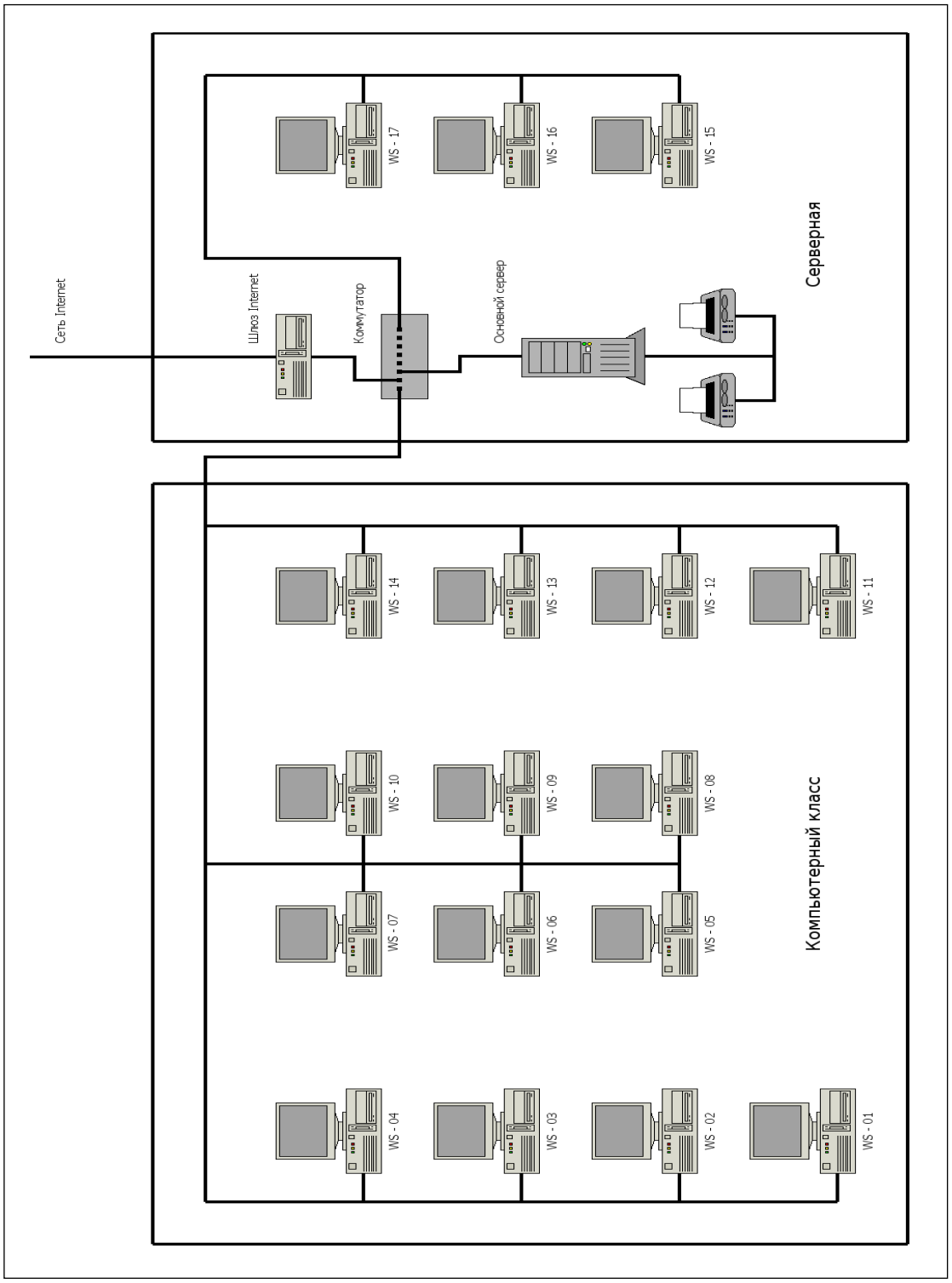

Рис. 1. Кафедральная локальная сеть

На данный момент ОС Windows XP используется на 3 рабочих станциях учебно-научного центра, при этом на этих рабочих станциях также установлена ОС Debian GNU/Linux. На всех остальных компьютерах используется только Debian GNU/Linux.

Центральной задачей основного сервера является предоставление санкционированного доступа ко всем сервисам учебно-научного центра. При этом необходимо было решить задачу создания единого центра авторизации пользователей для двух разнородных типов ОС: GNU/Linux и MS Windows. Для этого была использована база LDAP, хранящая все учетные записи пользователей.

ОС GNU/Linux позволяют использовать различные механизмы авторизации за счет применения технологий NSS (Name Service Switch) и PAM (Pluggable Authentication Modules). Для авторизации через базу LDAP были использованы модули libnss-ldap и libpam-ldap. Помимо авторизации, пользователям необходимо иметь доступ к своему домашнему каталогу, хранящемуся на сервере. Для этого используется сетевая файловая система NFS версии 3.

ОС семейства MS Windows используют доменную авторизацию, которая была реализована с использованием программы SAMBA, настроенной на использование базы LDAP. Также SAMBA используется как файловый сервер для доступа к домашним каталогам пользователей по протоколу CIFS. Таким образом, у пользователя имеется возможность с использованием единой учетной записи получить доступ ко всем рабочим станциям учебно-научного центра и своему домашнему каталогу, независимо от типа установленной или загруженной на данной рабочей станции ОС.

Кроме этого, имеется возможность получить безопасный доступ к домашнему каталогу пользователя из сети Интернет с использованием расширения протокола SSH (Secure Shell) — SFTP (Secure File Transfer Protocol). Во всех случаях для разграничения прав доступа к файлам используется стандартный механизм разграничения прав в системе GNU/Linux, а в особых случаях — расширенный метод Unix ACL (Access Control Lists).

Помимо авторизации и файлового хранилища, основной сервер предоставляет доступ к электронной почте, web-серверу и сетевым принтерам. Для проверки доступа к ним также используется база LDAP.

Электронная почта обеспечивает авторизованную отправку и прием писем по протоколам SMTP, IMAP и POP3. Уязвимым местом этих протоколов является передача учетных данных пользователя в открытом виде по сети. Для предотвращения перехвата этих данных связь с сервером осуществляется с использованием зашифрованного соединения SSL. Для этого на сервере используются программы Postfix и CourierIMAP.

Доступ к принтерам обеспечивает программа CUPS с использованием протокола IPP (Internet Printing Protocol).

Web-сервер обеспечивает работу сайта кафедры ЭФУ (www.accel.ru), на котором размещена учебная информация, программы для самостоятельного выполнения студентами лабораторных работ и портал дистанционного обучения. Работу web-сервера обеспечивает программа Apache.

Доступ к глобальной сети Интернет обеспечивает отдельный шлюз. В качестве шлюза в сеть Интернет используется компьютер с двумя сетевыми интерфейсами. Шлюз обеспечивает работу локальных компьютеров в сети Интернет с использованием механизма подмены адресов NAT (Network Address Translation), одновременно надежно защищая их от внешних воздействий. Для доступа к локальным ресурсам учебно-научного центра используется механизм Port Forwarding, который открывает доступ из внешней сети к IP-портам основного сервера, используемым для работы программ SSH, электронной почты и web-сервера. Работу NAT и Port Forwarding обеспечивает ядро ОС GNU/Linux.

Для обеспечения безопасности всего учебно-научного центра программы, доступ к которым возможен из сети Интернет, выполняются в изолированном окружении (chroot), что предотвращает доступ ко всей системе при взломе одной из них.

Программное обеспечение безопасности хранения информации, кроме традиционных средств ОС, включает средства инструментальной среды Moodle, на основе которой предполагается построение всех форм взаимодействия кафедральных циклов.

Можно выделить три уровня доступа к основным курсам кафедрального информационно-вычислительного центра: 1 — локальная сеть кафедрального компьютерного класса (20 ПК), в состав которого входит базовый UNIX-сервер (accel.ru), 2 — сеть кампуса МИФИ, включающая

компьютеры кафедральных учебно-исследовательских лабораторий, общеинститутские компьютерные классы, ПК студенческих общежитий и т. п., 3 — домашние компьютеры преподавателей и студентов, обучающихся в рамках учебных циклов кафедры. Каждый уровень доступа предполагает комплекс программно-аппаратных и административных мероприятий по защите как от преднамеренных, так и от непреднамеренных воздействий.

Что касается непреднамеренных воздействий, которые связаны с ошибками обслуживающего персонала, сбоями в электросети и т. п., то предусмотренная защита от них достаточно традиционна. Это прежде всего:

1. резервное копирование личных архивов пользователей (под ответственность пользователей), регулярное копирование наиболее важного и часто изменяемого как общеинститутского, так и прикладного ПО на различные внешние носители;

2. избыточность данных (обеспечивается как RAID-массивами центрального кафедрального сервера, так и отдельным резервным сервером (UNIX) в сети компьютерных классов МИФИ);

3. защита от сбоев в силовой сети (осуществляется общепринятыми средствами (UPS, SPS и т. п.)).

Основным средством защиты от нежелательных (преднамеренных) внешних воздействий является брандмауэр, представляющий комплекс программно-аппаратных средств, ограничивающих доступ к информационным ресурсам центра (см. на рис. 1 — шлюз-Internet). Связь с сервером осуществляется с использованием зашифрованного соединения SSL. Для этого используются программы Postfix и Courier IMAD.

Определенную роль в общем комплексе мер информационной безопасности играет Proxy схема с аутентификацией пользователей, которая создает соединение внешней сети (Интернет) с конечным адресатом через промежуточный сервер, и, таким образом, кафедральная локальная сеть ПК представляет приватную сеть с виртуальными IP-адресами.

2. Инструментальные средства дистанционного обучения

Включение в систему методов дистанционного обучения, связанного с удаленным доступом к web-серверу, обеспечивающему работу сайта кафедры ЭФУ (www.accel.ru), требует дополнительного администрирования и разграничения прав доступа для различных групп зарегистрированных пользователей, определяемых регламентом изучаемых курсов и порядком проведения лабораторных практикумов. Естественно, студенты допускаются только к своим личным архивам и методическим материалам изучаемых ими курсов. Преподаватели имеют как права доступа к архивам своих студентов, так и расширенные права к разработанным ими методическим материалам и средствам контроля за обучаемыми в течение семестра (тесты, критерии оценки знаний, журнал успеваемости и посещаемости и т. п.).

За основу инструментального ПО разработки портала дистанционного обучения принята виртуальная обучающая система Moodle [1], созданная в рамках проекта Collaboration Across Borders, получившего поддержку Европейской образовательной программы Socrates — Minerva.

Moodle — это программный продукт, базирующийся на Интернете (позволяющий создавать web-сайты), распространяется бесплатно в качестве программного обеспечения с открытым кодом (Open Sourse), работа в этой среде предполагает выполнение двух противоречивых требований. С одной стороны, открытость системы с предоставлением обширных возможностей сети Интернет — сотрудничество и дискуссии с другими пользователями, расширенные возможности изучаемого материала и конструирование собственных знаний, возможность загрузки дополнительных компонентов по изучаемой дисциплине, т. е. это web-технология, которая может использоваться как в режиме реального времени (on-line), так и в автономном режиме (off-line).

С другой стороны, система предоставляет права защиты от несанкционированного доступа — просмотра, а в ряде случаев и нарушения таких материалов, как тесты, критерии оценки знаний, журналы успеваемости и посещаемости в Сети и т. п. Как и любая защита, все эти мероприятия несколько снижают функциональность системы. Работа различных категорий пользователей строго регламентирована, права доступа к различным ресурсам системы устанавливаются авторизацией пользователей (каждый участник этой системы имеет свой логин и пароль, которые и определяют их возможности).

Безусловно, удаленный доступ студентов и преподавателей к информационным материалам по различным дисциплинам кафедры электрофизики и выполнение лабораторных практикумов «на дому» не являются альтернативой традиционным аудиторным занятиям, а служат лишь дополнительным средством расширения возможностей самостоятельной работы с использованием современных информационных и телекоммуникационных ресурсов глобальной сети Интернет.

В то же время внедрение этой системы позволяет повысить управляемость учебного процесса и степень объективности оценки работы и знаний студентов преподавателями. Текущая информация об «активности» студентов и результативности их работы, степени освоения курса, оценка знания на текущий момент, затраченное время, количество посещений (выход на сайт) сохраняются в базе данных в течение всего времени аудиторных занятий по соответствующему курсу.

Безусловно, каждый разработанный в среде Moodle курс требует индивидуальной проработки, оценки целесообразности выбора различных функций среды (глоссарий, ресурс, задание, форум, урок, тест и т. д.).

3. Примеры использования разрабатываемых средств в учебном процессе кафедры

На начальном этапе эта система была опробована на нескольких компьютерных практикумах кафедры. Первыми в систему были включены практикумы по курсу САПР ЭФУ. Один из них — практикум по решению задач электрофизики в системе MatLab [2] — связан с изучением возможностей и приобретением навыков работы в среде одного из наиболее популярных и адаптированных к характерным задачам ЭФУ и ускорительной техники пакета прикладных программ (ППП) MatLab. Тематика заданий связана с расчетом статических и динамических электромагнитных полей в ускоряющих и фокусирующих системах различной конфигурации и оптимизацией этих структур. Не менее важной задачей расчета является также исследование устойчивости и группировки частиц в этих полях.

Хотя MatLab может рассматриваться как язык сверхвысокого уровня, в значительной степени исключающий рутину традиционного программирования и позволяющий сосредоточиться на конкретных физических задачах, тем не менее специфика используемых в языке объектов данных, обширные функциональные возможности и особенности интерфейса требуют определенного времени для самостоятельного освоения пакета. В связи с этим удаленный доступ к данному лабораторному практикуму оказывается как нельзя кстати.

Фрагменты выполняемых студентами задач по исследованию электростатических и высокочастотных полей представлены на следующих рисунках. На рис. 2 приведены конфигурации полей для системы двух зарядов одного знака и системы двух зарядов разных знаков.

На рис. 3 приведены силовые линии волны типа H_{mn} в прямоугольном волноводе. Решение приведенной системы уравнений дает аналитические зависимости силовых линий электрического (а) и магнитного (б) полей в поперечном и продольном сечении прямоугольного волновода.

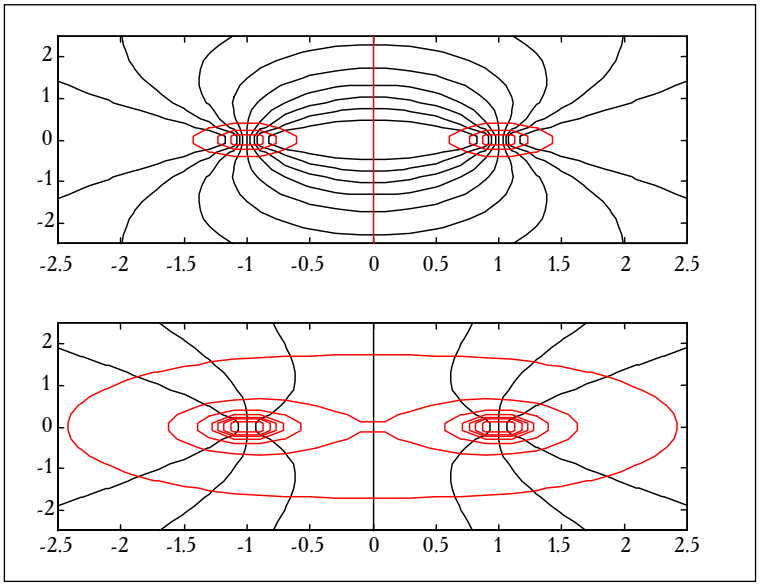

Рис. 2. Конфигурация полей

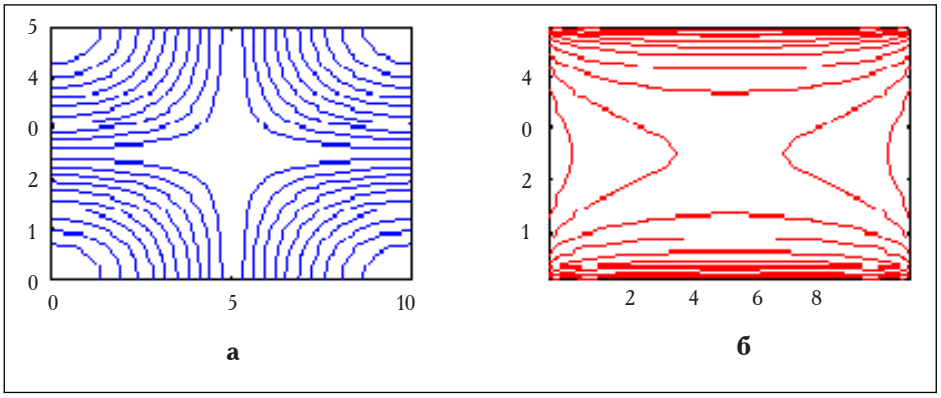

Рис. 3. Силовые линии волны в прямоугольном волноводе

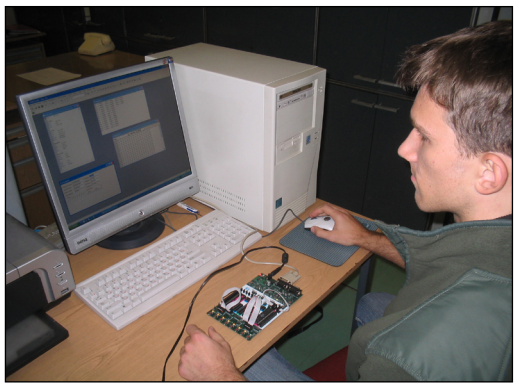

Рис. 4. Физическое моделирование микроконтроллера

Необходимо отметить, что включение элементов дистанционного обучения не ограничивается только расчетно-теоретическими практикумами ЭФУ. Так, в традиционно экспериментальной учебной лаборатории «Электронные системы ускорителей» в разделе «Микропроцессорные системы ЭФУ» наряду с экспериментальными измерительными стендами (Рис. 4), на которых студенты приобретают опыт работы с микроконтроллерами семейства ATMEL AVR, используется программная модель микропроцессора этого контроллера (симулятор), которая позволяет проводить

исследования, программировать и разрабатывать реальные системы управления вне лабораторного практикума (в том числе и с использованием «домашних» компьютеров) (Рис. 5).

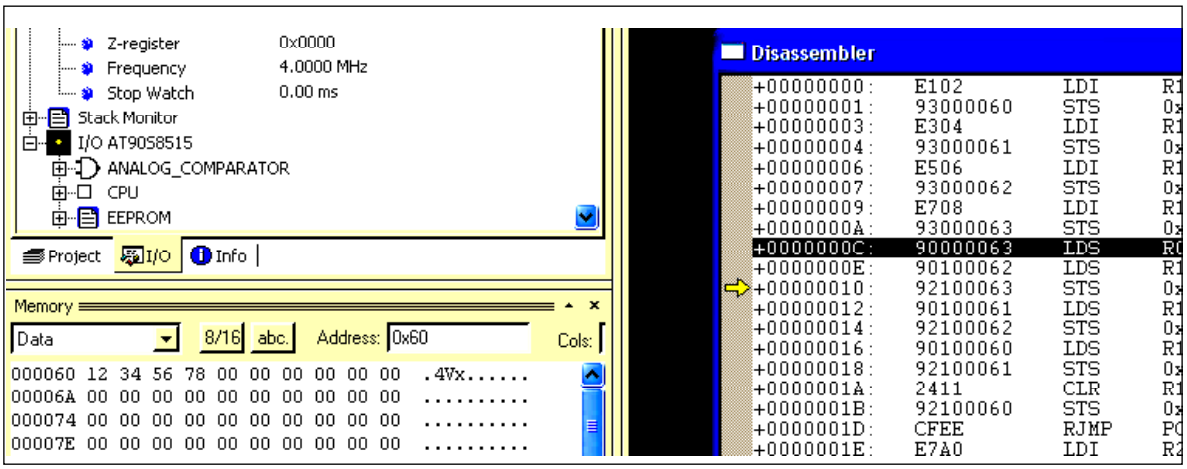

Рис. 5. Среда разработки приложений AVR Studio

Подобные возможности — в стадии разработки и внедрения в практику учебных лабораторий по мощной импульсной технике, вакуумной технике и физической электронике.

В заключение следует отметить:

1. Опытная эксплуатация кафедрального информационно-вычислительного центра в режиме аудиторных занятий (включая общеинститутские компьютерные классы) по курсам «Информатика» и «САПР ЭФУ» оказалась вполне успешной и предполагает дальнейшее развитие — включение всех кафедральных циклов занятий.

2. Включение на входе в кафедральную ЛВС брандмауэра и переход на среду ОС GNU/Linux значительно повысил защищенность информационных ресурсов сетевого сервера как от внешних воздействий, так и от несанкционированных внутренних взаимодействий.

3. Включение в систему элементов дистанционного обучения хотя и находится на начальном этапе своего развития, встречено с большим энтузиазмом студентами, часть из которых участвует в ее разработке.

СПИСОК ЛИТЕРАТУРЫ:

1. Open Sourse Conrse Management System. URL: http://moodle.org/.
2. *Потемкин В. Г.* Система инженерных и научных расчетов MATLAB 5.x. Т. 1, 2. М.: Диалог МИФИ, 1999.