



ИБ В СФЕРЕ ОБРАЗОВАНИЯ

БИТ

А. И. Гусева, В. С. Киреев, С. А. Филиппов, А. С. Цыплаков

ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНЫЙ ПОРТАЛ МИФИСТ: ПОЛИТИКА БЕЗОПАСНОСТИ ПРИ РАЗГРАНИЧЕНИИ ДОСТУПА К ОБЪЕКТАМ

Введение в проблему

В рамках реализации ИОП МИФИ в 2008 г. введен в опытную эксплуатацию информационно-образовательный портал МИФИСТ для поддержки самостоятельной работы студентов, реализующий такие инновационные составляющие инженерного образования, как активные формы обучения, возможность создания индивидуальных образовательных траекторий и дистанционная поддержка учебного процесса. В основу разработки были положены требования интеграции информационных ресурсов нескольких десятков учебных заведений по всей стране, которые вошли в состав Национального исследовательского ядерного университета «МИФИ» [1–3].

Цель реализации инновационной образовательной программы состояла в развитии инженерно-физического образования для подготовки специалистов по критическим технологиям, обладающих фундаментальными знаниями, высокой профессиональной компетентностью и умением превращать знания в инновации. В этих условиях научно-техническая и методическая оснащенность МИФИ должна быть приведена в состояние, адекватное состоянию лучших университетов Европы, Америки и Азии, готовящих специалистов по ядерной физике и технологиям. Одним из важных факторов, определяющих переоснащение учебно-методической базы, является расширение информационно-образовательной среды МИФИ за счет включения в нее дополнительных возможностей, связанных с поддержкой активных форм обучения и самостоятельной работы студентов.

Все вышесказанное определяет особую актуальность создания информационно-образовательного портала поддержки самостоятельной работы студентов для внедрения инновационных технологий в область инженерно-физического образования на новом этапе развития ядерной науки и промышленности.

Назначение и архитектура портала МИФИСТ

Система МИФИСТ предназначена для организации информационно-образовательного пространства для самостоятельной работы студентов и создание хранилища учебно-методических материалов. Разработка системы сопровождалась созданием информационного, программного, методического и организационного обеспечения образовательного портала для последующего постепенного наполнения его информационными ресурсами и учебными элементами. Разработанная

система обеспечивает автоматизированное выполнение функций публикации информационных и учебных материалов преподавателями, доставки учебных материалов учащимся, сбора и оценки выполненных студентами самостоятельных работ разного рода, сбора и обработки различных статистических отчетов.

Работа пользователей в системе МИФИСТ контролируется подсистемой мониторинга, которая представляет информацию о событиях в виде пользовательских логов. Логи показывают, когда, какой именно пользователь совершал действия в системе, сколько времени он затратил на выполнение тех или иных учебных заданий и тестов, на чтение информационных ресурсов и т. д. На основе анализа логов происходит мониторинг деятельности пользователей системы.

Мониторинг деятельности учащихся может проводиться по следующим видам отчетов:

- доступ к ресурсам (гlossариям, конспектам лекций и т. д.);
- результаты выполнения контролируемых элементов (автоматическая проверка);
- результаты выполнения заданий, рабочих тетрадей, семинаров, групповых проектов (автоматизированная проверка);
- формирование рейтинга учащегося.

Система МИФИСТ обладает трехуровневой архитектурой и состоит из следующих подсистем. На первом уровне находится подсистема «Учебное управление»; на втором уровне — «Факультет» (8 клонов, на каждый факультет МИФИ); на третьем уровне находятся подсистемы «Кафедра» (80 клонов, на каждую кафедру МИФИ по одному), «Портфолио студента» (8112 экземпляров, для каждого студента); «Личный кабинет преподавателя» (1430 экземпляров, для каждого преподавателя); подсистема «Хранилище учебных материалов».

Основным назначением подсистемы «Учебное управление» является сбор, обработка и организация доступа к информации на уровне института о самостоятельной работе студентов; создание статистических отчетов по каждому факультету, кафедре, учебной группе, студенту, преподавателю, учебной дисциплине МИФИ; доступ к оперативной информации по каждому факультету, кафедре, учебной группе, студенту, преподавателю, учебной дисциплине МИФИ; предоставление другим подсистемам информации о семестровых учебных планах, списки кафедр, факультетов, студентов и преподавателей, результаты сессий в формате MS Excel.

К функциям подсистемы «Факультет» относятся: сбор и обработка статистической информации по отдельному факультету, кафедре, учебной группе, студенту, преподавателю, учебной дисциплине; создание статистических отчетов; доступ к оперативной информации; предоставление другим подсистемам соответствующей информации.

Подсистема «Кафедра» несет основную нагрузку по организации самостоятельной работы студентов, сбору, обработке и доступу к информации на уровне каждой кафедры. К функциям подсистемы относятся:

- публикация информационных и учебных материалов, а также контролируемых учебных элементов; доступ к учебным материалам, доставка учебных материалов учащимся, оценка результатов самостоятельной работы студентов и вычисление рейтинга, сбор и обработка статистической информации по отдельной кафедре, учебной группе, студенту, преподавателю, учебной дисциплине факультета, создание статистических отчетов по кафедре, учебной группе, студенту, преподавателю, учебной дисциплине факультета, доступ к оперативной информации по кафедре, учебной группе, студенту, преподавателю, учебной дисциплине факультета, предоставление другим подсистемам информации (списки кафедр, факультетов, студентов и преподавателей, результаты сессий в формате MS Excel).

Электронные учебные элементы (создаваемые, модифицируемые и удаляемые) составляют основное учебно-методическое обеспечение системы МИФИСТ. Высокая трудоемкость



создания таких элементов может частично компенсироваться их наглядностью, многократной используемостью и возможностью тиражировать подготовленные материалы в разных формах.

Это существенно упрощает отбор, обработку и организацию доступа к информации о дисциплинах текущего семестра, которые проводит конкретный преподаватель. Подсистема предоставляет доступ к оперативной информации по учебным дисциплинам текущего семестра для ведения занятий отдельным преподавателем, возможность сбора и обработки статистической информации по результатам выполнения текущих самостоятельных заданий студентами, информацию о текущих результатах студентов другим подсистемам (в формате MS Excel).

Подсистема «*Портфолио студента*» предназначена для сбора, обработки и организации доступа к информации о самостоятельных заданиях в рамках дисциплин текущего семестра, которые должен выполнить студент. Подсистема предоставляет доступ к оперативной информации по учебным дисциплинам текущего семестра для отдельного студента, возможность сбора и обработки статистической информации по результатам выполнения текущих самостоятельных заданий, информацию о текущих результатах студента другим подсистемам (в формате MS Excel).

Назначением подсистемы «*Хранилище*» является импорт, хранение и экспорт архивированных учебных материалов. Подсистема обеспечивает импорт из подсистемы «*Кафедра*» архивированных учебных материалов после окончания учебного семестра (дважды в год), каталогизацию учебных материалов, доступ к каталогизированным материалам, экспорт в подсистему «*Кафедра*» архивированных материалов.

Характеристики системы МИФИСТ

В основу проекта системы МИФИСТ заложены следующие характеристики: масштабируемость, производительность, надежность, открытость, переносимость, совместимость по данным с существующими БД МИФИ, безопасность.

Масштабируемость системы на первом этапе была рассчитана на 14 000 пользователей. Система функционирует на базе локальной сети МИФИ и обеспечивает не менее 1000 одновременных подключений. В дальнейшем, при подключении дополнительных серверов, нагрузка системы может возрасти до 30 000 пользователей.

Открытость системы МИФИСТ означает, что проектирование системы проведено по модульному принципу, который позволяет расширять и модифицировать функционал подсистем.

Конфигурация жестких дисков системы МИФИСТ позволяет создать массивы RAID-5 для увеличения быстродействия без потери защищенности от технических неисправностей при выходе из строя одного из жестких дисков в каждом RAID-массиве. Система резервирования данных позволяет быстро восстановить системные файлы и файлы данных с оптического накопителя.

Переносимость программного обеспечения означает, что в качестве серверной платформы может использоваться как Windows 2003 Server с соответствующим IIS, так и свободно распространяемый программный код ОС FreeBSD с Apache + PHP Mod.

Использование в качестве ядра системы МИФИСТ свободно распространяемого программного кода (e107, LMS Moodle) позволило обеспечить лицензионную чистоту разработки.

Совместимость по данным с существующими базами данных, в первую очередь с системой «АСУ-Деканат» версии 2007 г., обеспечивается через формат Excel-файлов.

Система информационной безопасности

Для любой реализации портала жизненно важно гарантировать, что получаемые с его помощью информация, службы и метаданные безопасны и что доступ к ним имеют лишь те пользователи, которые обладают соответствующими правами. Важным моментом реализации портала является организация аутентификации пользователей и система администрирования прав доступа как отдельных пользователей, так и групп пользователей, объединенных ролями. Важно



также, чтобы портал поддерживал единую точку входа и не требовал у пользователей предоставлять реквизиты при обращении к каждому хранилищу информации или службе.

В отношении безопасности информации система МИФИСТ обеспечивает:

- идентификацию, проверку подлинности и контроль доступа пользователей в систему;
- регистрацию входа и выхода пользователей из системы;
- разграничение доступа к различным функциям и данным.

Средства, поддерживающие информационную безопасность, используются на трех уровнях защиты: серверной операционной системы, приложения в виде интернет-сервера и самой системы МИФИСТ. Такая комплексная защита обеспечивает целостность, конфиденциальность и доступность информации, а также безопасность использования. В качестве организационных мер защиты предусмотрено отдельное помещение с ограниченным доступом

В целом ситуация осложняется тем, что портал строится с помощью продуктов разных производителей. В этом случае сложность создания и поддержки единой и непротиворечивой подсистемы аутентификации и авторизации пользователей на портале становится очень высокой, если не использовать для этого программный продукт или подсистему с унифицированным интерфейсом управления.

В данном случае наилучшим решением является построение своей надежной системы аутентификации, полностью интегрированной в структуру портала, заведомо обеспечивающую надлежащий доступ к portalу и эффективное администрирование.

На основе требований к информационно-образовательному portalу были определены следующие наборы прав для управления правом доступа к объектам, их свойствам и данным:

- b = просмотр объектов и их свойств (browse)
- c = создание объекта (create)
- m = изменение свойств объекта (modify)
- e = удаление объекта (erase)
- p = изменение прав доступа к объекту (permission)
- r = чтение данных (read)
- a = добавление данных (add)
- w = изменение данных (write)
- d = удаление данных (delete)
- i = наследуемость (inheritable)

Наборы $\alpha = \{b, c, m, e, p\}$ и $\beta = \{r, a, w, d, i\}$ обладают функциональной полнотой, так как полностью покрывают все потребности в обращении с объектами, их свойствами и данными, что доказывается с помощью соответствующей семантической таблицы покрытий (таблица 1):

Таблица 1. Права доступа к объектам, их свойствам и данным

Действия	Права доступа									
	b	c	m	e	p	r	a	w	d	i
Над объектами										
Просмотр	1									
Удаление				1						
Создание		1								
Изменение прав доступа					1					
Над свойствами										
Просмотр	1									



Изменение			1							
Над данными										
Чтение						1				
Добавление							1			
Изменение								1		
Удаление									1	
Наследуемость										1

Политика безопасности должна включать в себя, по крайней мере, следующие элементы:

- произвольное управление доступом;
- безопасность повторного использования объектов;
- метки безопасности;
- принудительное управление доступом.

Произвольное управление доступом — это метод ограничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо может по своему усмотрению давать другим субъектам или отбирать у них права доступа к объекту. Большинство операционных систем и систем управления базами данных реализуют именно произвольное управление доступом. Главное его достоинство — гибкость, главные недостатки — распределенность управления и сложность централизованного контроля.

Безопасность повторного использования объектов — важное на практике дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения секретной информации из «мусора». Безопасность повторного использования должна гарантироваться для областей оперативной памяти, в частности для буферов с образами экрана, расшифрованными паролями и т. п.

Для реализации принудительного управления доступом с субъектами и объектами ассоциируются метки безопасности. Метка субъекта описывает его благонадежность, метка объекта — степень закрытости содержащейся в нем информации. Согласно «Оранжевой книге», метки безопасности состоят из двух частей: уровня секретности и списка категорий. Принудительное управление доступом основано на сопоставлении меток безопасности субъекта и объекта. В целях обеспечения требуемого уровня безопасности в системе МИФИСТ используется принудительное управление доступом к объектам.

На основе референтных моделей ролей в соответствии с международным стандартом IEEE для систем дистанционного образования были реализованы и настроены функциональные профили ролей, которые исполняются в системе МИФИСТ: «Наблюдатель», «Редактор», «Администратор контента» (информационный администратор), «Администратор», «Студент», «Преподаватель». Система безопасности обеспечивает разграничение доступа к ресурсам в соответствии с назначенной ролью.

Роль «Наблюдатель» присутствует во всех подсистемах на всех трех уровнях иерархии системы МИФИСТ. Она предназначена для мониторинга и контроля соответствующих процессов. Функции, которые исполняет «Наблюдатель», заключаются в формировании всевозможных статистических отчетов и выводе их на печать.

Роль «Редактор» присутствует только в подсистемах «Учебное управление» и «Факультет». Она предназначена для ввода или коррекции данных по факультетам, кафедрам, дисциплинам, преподавателям, студентам.



Роль «Информационный администратор» присутствует только в подсистеме «Кафедра», необходима для наполнения соответствующими информационными и учебными материалами кафедральных рубрик.

Роль «Студент» присутствует в двух подсистемах: «Кафедра» и «Портфолио студента», предназначена для обучения. Процесс обучения заключается в просмотре информационных и учебных материалов, а также в выполнении тестов, заданий, заполнении опросов, рабочих тетрадей и т. д. Помимо этого, возможно создание и отправка сообщений на форум, чат или по электронной почте.

Роль «Преподаватель» создана для трех подсистем: «Хранилище», «Кафедра» и «Личный кабинет преподавателя» — и предназначена как для проведения занятий, так и для создания учебных элементов. Помимо этого, из подсистемы «Хранилище» «Преподаватель» может проводить восстановления данных в подсистему «Кафедра».

На роль «Администратор» возлагаются функции по управлению пользователями, кафедрами, факультетами, курсами, привязке заданий к учебному плану студента, формированию учебной нагрузки преподавателя, архивированию и восстановлению данных. Данная роль существует во всех подсистемах.

Введение дополнительного правила в политику безопасности, ограничивающего множество прав для субъектов, исполняющих роли «Студент» и «Наблюдатель», повышает уровень защиты информации в системе МИФИСТ. Для «Наблюдателя» назначены ограниченные подмножества прав $\varepsilon = \{b\} \in \alpha$ и $\phi = \{r\} \in \beta$. Для «Студента» эти права составляют $\varepsilon = \{b\} \in \alpha$ и $\phi = \{r\} \vee \{r, a\} \in \beta$.

Для настройки ролей «Администратор», «Преподаватель», «Информационный администратор», «Редактор» разрешается использование любых подмножеств наборов прав α и β .

В этом случае полные права (γ) на указанный объект и его данные вычисляются по формуле (1).

$$\gamma = \sum_A \varepsilon + \sum_B \sum_i \alpha_i + \phi_A + \beta_B \quad (1)$$

Таким образом, система МИФИСТ обеспечивает разграничение доступа к ресурсам в соответствии с математической моделью организации авторизованного доступа в разнородных распределенных образовательных веб-ориентированных системах.

Заключение

Внедрение в учебный процесс системы МИФИСТ (за 2007/2008 г.) привело к созданию большого объема учебно-методического наполнения общеобразовательных и специальных дисциплин по ряду инженерных специальностей, в том числе связанных с ядерными технологиями. В настоящее время система МИФИСТ развернута в 80 различных подразделениях НИЯУ МИФИ и имеет наполнение в виде 50 учебно-методических комплексов по дисциплинам и 70 различных тематических баз данных тестовых вопросов (объемом 5000 вопросов) и обслуживает 8500 студентов и 1500 преподавателей НИЯУ МИФИ.

Использованные политики безопасности в отношении доступа к объектам показали свою работоспособность и надежность. За время трехлетней обработки большого количества ежедневных пользовательских запросов объемом в десятки тысяч единиц на авторизацию и доступ к ресурсам не зафиксировано ни одного сбоя в системе безопасности информационно-образовательного портала МИФИСТ.

Впоследствии опыт использования системы МИФИСТ позволил заменить два уровня архитектуры информационной системой управления учебной деятельностью, оставив за системой МИФИСТ функции электронного обучения.



Перспективы развития системы МИФИСТ могут быть сформулированы следующим образом.

- Система МИФИСТ является элементом единого образовательного пространства НИЯУ МИФИ.

- С ее помощью может быть организовано дистанционное обучение для унификации образовательных программ для всех удаленных подразделений НИЯУ МИФИ; в настоящее время в системе МИФИСТ проходят апробацию такие дистанционные курсы в формате SCORM 2004, как «Математика» (1 семестр), «Физика» (1 семестр) и «Химия» (1 семестр).

- С использованием системы МИФИСТ может быть организовано фронтальное тестирование по основным общеобразовательным дисциплинам. При подготовке к фронтальному интернет-тестированию в 2009/2010 г. систему использовали более 20 кафедр НИЯУ МИФИ по 34 дисциплинам.

- В области повышения квалификации по таким приоритетным направлениям, как «Проблемы информатизации образования», «Информационная компетентность в профессиональной деятельности преподавателя вуза», «Развитие новых форм и технологий повышения квалификации ППС (дистанционные и модульные технологии)» и «Современные технологии обучения», обучение с помощью системы МИФИСТ прошли 580 преподавателей НИЯУ МИФИ и 223 преподавателя из 80 вузов России.

- Результаты апробация методик и технологий обучения, предложенных преподавателями в процессе повышения квалификации, опубликованы в системе МИФИСТ по адресам portelai.mephi.ru/atom и portelai.mephi.ru/iop.

Система МИФИСТ зарегистрирована в установленном порядке в Объединенном фонде электронных ресурсов «Наука и образование» [4].

СПИСОК ЛИТЕРАТУРЫ:

1. Гусева А. И., Харитонов В. В., Кербель Б. М. и др. Корпоративный ядерный университет: предпосылки, концепция, структура. Северск: СГТИ, 2004. – 138 с.
2. Гусева А. И., Киреев В. С., Тихомирова А. Н., Филиппов С. А. Компетенции работников образования в области информационных и коммуникационных технологий. Монография. М.: МИФИ, 2009. – 256 с.
3. Гусева А. И., Киреев В. С., Тихомирова А. Н., Филиппов С. А., Цыплаков А. С. Информационно-образовательный портал МИФИСТ исследовательского ядерного университета // Программные продукты и системы. 2009. № 3. С. 57–62.
4. Гусева А. И., Киреев В. С., Маслий Н. П., Тихомирова А. Н., Цыплаков А. С., Цыганов А. А., Филиппов С. А. Свидетельство о регистрации электронного ресурса «Автоматизированная обучающая система «Система поддержки самостоятельной работы студентов МИФИСТ». М.: РАО, ОФЕРНиО, Свидетельство о регистрации электронного ресурса № 15417 от 03 марта 2010 г. Инв. номер ВНТИЦ № 50201000336 от 09.03.2010 г.