

УДК 004.853

Н.В. Суханова

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ДИСТАНЦИОННОГО ОБУЧЕНИЯ В ТЕХНИЧЕСКИХ ВУЗАХ НА БАЗЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Сформулированы требования к системе дистанционного обучения в технических вузах. Разработана архитектура системы дистанционного обучения на основе критического анализа аналогичных систем.

Ключевые слова: дистанционное обучение, защита информации, искусственный интеллект, искусственные нейронные сети.

Развитие информационных технологий создает предпосылки для совершенствования традиционных и разработки новых форм обучения, в частности дистанционного обучения.

Дистанционная форма обучения – это новая форма обучения, когда для обеспечения учебного процесса используются современные информационные технологии и Интернет. Такая форма обучения актуальна для нашей страны из-за протяженной территории, наличия отдаленных населенных пунктов, неритмичной и неэффективной работы транспорта. Система дистанционного обучения привлекает в вуз людей, у которых работа имеет разъездной характер, связана с частыми командировками, а также желающих получить высшее образование, но не имеющих финансовых возможностей для обучения в вузе с отрывом от производства. Отдельные элементы системы дистанционного обучения можно использовать при очной, вечерней и заочной формах обучения. Например, в режиме дистанционного обучения могут проходить факультативные занятия, могут преподаваться отдельные дисциплины вариативной части (по выбору студентов), если группа малочисленная или если временно отсутствует штатный преподаватель.

Система дистанционного обучения должна отвечать всем требованиям, предъявляемым к высшим учебным заведениям, а также включать следующие дополнительные возможности, которые дают современные информационные технологии и Интернет:

- учебно-методические материалы должны быть представлены в электронном виде с возможностью их представления на сайте и передачи по сети Интернет;
- практические занятия должны включать пошаговый разбор и анализ решений типовых задач, контрольные работы, тесты, рефераты и доклады по выбранной теме;
- лабораторные работы должны проходить в режиме моделирования или включать работу на оборудовании в удаленном режиме;
- контроль времени дистанционного обучения;
- применение средств автоматизированного контроля и оценки знаний.

Система дистанционного обучения должна иметь развитую систему администрирования, позволяющую:

- распределять права доступа пользователей;
- хранить результаты обучения студентов;
- обеспечивать защиту информации от третьих лиц.

Таким образом, дистанционное обучение ставит новые задачи:

- защиты информации при хранении на общедоступном сайте и передаче по открытым каналам связи;
- одновременной идентификации и аутентификации большого числа пользователей, разграничения прав пользователей;
- доступности информации для большого числа пользователей;
- выполнения лабораторных работ в удаленном режиме или с помощью моделирования;

- дистанционного контроля и оценки знаний;
- оценки эффективности работы системы дистанционного обучения и др.

Возможности искусственных нейронных сетей (ИНС) намного шире, чем задачи обучения. Традиционные ИНС позволяют лишь частично, неполно и приближенно моделировать отдельные функции мозга человека.

При создании нейронных сетей с большим числом нейронов возникают две основные проблемы:

- большого числа взаимных связей нейронов в сети;
- времени обучения большой нейронной сети.

Автором была разработана новая коммутаторная и доменная архитектура построения больших искусственных нейронных сетей [3; 4]. Эта архитектура позволяет строить большие нейронные сети особого вида, по числу нейронов сопоставимые с мозгом человека. Проблема взаимных связей нейронов решается путем добавления в ИНС устройств для реализации взаимных связей нейронов - коммутаторов. После добавления коммутаторов традиционную нейронную сеть преобразуют к эквивалентному виду, с древовидной иерархической структурой. Взаимные связи большого числа нейронов реализованы путем каскадного соединения коммутаторов.

Проблема времени обучения нейронной сети решается двумя путями:

1. Большую нейронную сеть разделяют на фрагменты меньшего размера. Крупные фрагменты ИНС с большим числом нейронов делят на несколько мелких фрагментов. Проводят обучение отдельных мелких фрагментов. Обученные мелкие фрагменты объединяют в крупные, затем проводят их дополнительное обучение на основе традиционных методов.

2. Используется нейронная сеть особого вида, которая разделена на параллельные слои [8]. Обучение первого слоя ИНС проводят на основе традиционных методов. Добавляют еще один слой и проводят дополнительное обучение на основе генетических алгоритмов. Слои добавляют последовательно, пока выходные сигналы отличаются от эталона, заданного в обучающей выборке. Число слоев заранее не известно и зависит от заданной точности выходных данных.

Разработка архитектуры системы дистанционного обучения. На основе критического анализа аналогичных систем была разработана архитектура системы дистанционного обучения на базе ИНС (таблица).

За основу была принята клиент-серверная архитектура [1] с тонким клиентом, когда основная часть информации и программных средств системы дистанционного обучения хранится на сервере (рис. 1, 2). При такой архитектуре к клиентской части не предъявляют специальных требований по производительности процессора, объему памяти и т.д. В качестве клиента может использоваться не только настольный персональный компьютер или ноутбук, но и планшет или смартфон. На клиентском компьютере устанавливается специальное программное обеспечение, которое предназначено для поддержки режима дистанционного обучения и моделирования простых ИНС с небольшим числом нейронов.

На сервере устанавливается программное обеспечение, которое предназначено для поддержки режима дистанционного обучения и моделирования больших ИНС.

Идентификация, аутентификация пользователей и защита информации в системе дистанционного обучения. Обмен информацией между компьютерами-клиентами и сервером происходит по открытым общедоступным каналам связи. В разработанной системе дистанционного обучения использован новый метод идентификации, аутентификации пользователей и криптографической защиты информации [9; 10]. При идентификации пользователя выполняется ввод его личных данных и регистрация клиентского ком-

пьютера в системе дистанционного обучения. После регистрации пользователь получает уникальный секретный ключ.

При аутентификации пользователь вводит личные данные с клиентского компьютера. Клиент формирует и отправляет запрос на сервер.

Таблица

Сравнительный анализ различных вариантов архитектуры системы дистанционного обучения

| Архитектура системы дистанционного обучения | Достоинства | Недостатки |
|---|--|---|
| Централизованная система и терминалы пользователей | Большая производительность. Возможность реализовать сложные модели | Высокая цена. Отказ центрального компьютера приводит к отказу системы |
| Децентрализованная система на базе персональных компьютеров и Интернета | Низкая цена. Доступность | Ограниченные вычислительные возможности персональных компьютеров. Реализация только простых моделей |
| Клиент-серверная архитектура с толстым клиентом | Возможность моделирования в режиме реального времени. Возможность изменять параметры и структуру моделей | Ресурсы клиента не позволяют моделировать большие ИНС |
| Клиент-серверная архитектура с тонким клиентом | Возможность реализации моделей с разным уровнем сложности | Необходимость параллельной обработки на сервере запросов от большого числа клиентов |
| Разработанная клиент-серверная архитектура на базе ИНС | Реализация моделей с разным уровнем сложности на базе ИНС | Сложность реализации больших ИНС |

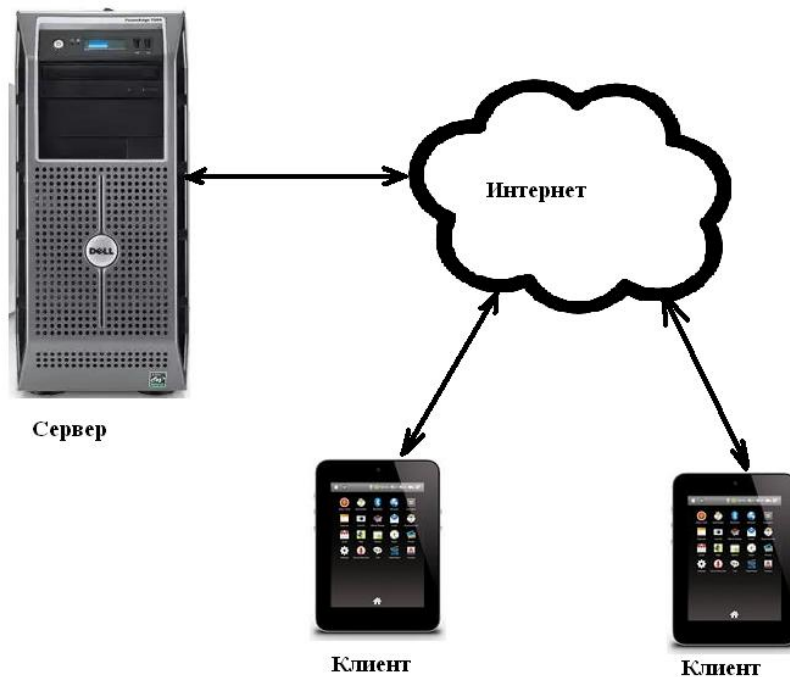


Рис. 1. Клиент-серверная архитектура системы дистанционного обучения

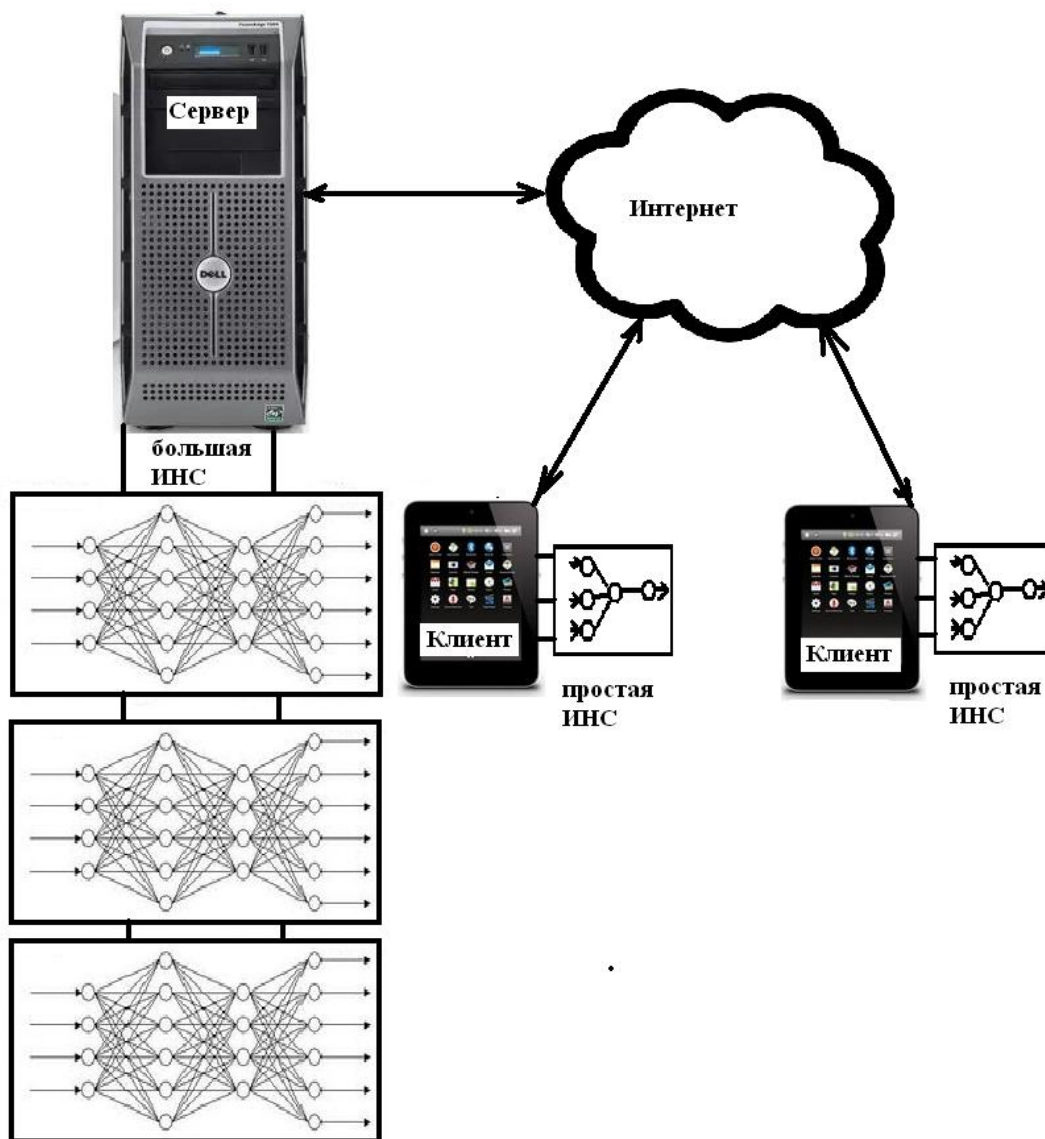


Рис. 2. Разработанная архитектура системы дистанционного обучения на базе ИНС

Для защиты информации в системе дистанционного обучения использован метод блочной шифрации с переменным ключом, который состоит в следующем. Информация разделяется на блоки. При обмене данными клиента с сервером каждый блок данных шифруется новым уникальным подключом. Подключ получают путем преобразования и модификации исходного секретного ключа пользователя. При модификации ключа используют личные данные пользователя и его компьютера, а также генератор псевдослучайных чисел. При переносе клиентской части на другой компьютер система выполняет перерегистрацию пользователя и создает новый (другой) секретный ключ. Таким образом, метод криптографической защиты информации на компьютере клиентской части исключает возможность несанкционированного доступа к информации, ее копирования, тиражирования и использования на другом компьютере.

На сервере создана база данных (БД), которая хранит следующую информацию:

- информацию о пользователе;
- информацию о компьютере клиентской части;
- секретный ключ пользователя;

- текущий секретный блочный подключ;
- результаты обучения пользователя.

Записи в БД хранятся в зашифрованном виде и доступны только конкретному пользователю для просмотра или системному администратору для контроля.

При потере секретного ключа (например, при отказе клиентского компьютера) легальный пользователь может провести генерацию нового секретного ключа на другом компьютере и восстановить все данные и программное обеспечение клиентской части.

На сервере периодически создается резервная копия всей информации. При отказе сервера информация восстанавливается по ее резервной копии.

База данных сервера реализована как устройство ассоциативной памяти [2; 5], которое включает большую обученную ИНС. В ИНС данные хранятся в зашифрованном виде. Перед записью данных в ассоциативную память выполняется их шифрация секретным ключом пользователя. На вход шифратора поступает информация и секретный ключ. На выходе шифратора формируется информация в зашифрованном виде. Выход шифратора подключен к ассоциативной памяти.

Таким образом, информация хранится на сервере и передается по открытым каналам связи через Интернет в зашифрованном виде (рис.2).

В клиентском компьютере информация хранится в зашифрованном виде. Дешифрацию информации проводят секретным ключом пользователя. Для отображения данных на экране клиентского компьютера их преобразуют в форму, удобную для восприятия человеком.

В случаях несанкционированного доступа к ассоциативной памяти на сервере, перехвата блоков данных при передаче через Интернет, копирования файлов с клиентского компьютера третьим лицам будет доступна только информация в зашифрованном виде.

В процессе работы в систему дистанционного обучения добавляют новых пользователей. Сведения об обучении зарегистрированных пользователей постоянно обновляются. Таким образом, в ассоциативной памяти необходимо использовать ИНС специального вида, которые позволяют проводить обучение и менять связи между нейронами в процессе их работы. Ассоциативная память реализована как модульная вычислительная система на базе многослойной ИНС [7; 8] и содержит слои, зашифрованные разными личными ключами пользователей.

Модель для выполнения лабораторных работ на базе ИНС. Для дистанционного выполнения лабораторных работ применяются следующие методы:

1. Моделирование оборудования.
2. Дистанционный доступ к оборудованию.
3. Комбинация первого и второго методов.

Предлагается проводить лабораторные работы в режиме моделирования реального оборудования. Модель реализована на базе многослойной модульной вычислительной системы, где модули содержат фрагменты ИНС [3-5; 7; 8].

Модель для выполнения лабораторных работ состоит из модели лабораторного стенда и модели оборудования и внешней среды. Модель внешней среды реализует физические процессы, протекающие в среде, где работает реальное оборудование. Модель лабораторного стенда выполнена в виде графического конструктора, где пользователь может реализовать любую возможную схему путем выбора и взаимного соединения стандартных элементов.

Модель лабораторных работ разработана с использованием клиент-серверной архитектуры и позволяет клиенту посылать запросы на сервер. Программа, моделирующая лабораторный стенд, находится на компьютере пользователя. Программа, моделирующая оборудование и внешнюю среду, находится на сервере. После обработки полученных запросов сервер отправляет результаты на компьютер пользователя. Такой системе дистан-

ционного обучения не требуются большие вычислительные возможности компьютера пользователя.

Большая часть лабораторной работы проводится на клиентском компьютере пользователя, где реализована модель лабораторного стенда. Все сложные вычисления выполняются на сервере. Клиентская часть обращается к серверу только после контроля, проверки и испытаний модели лабораторного стенда. Сервер должен обладать высокой вычислительной мощностью и возможностью параллельной обработки запросов от многочисленных клиентов. На сервере реализована большая обученная ИНС с многослойной модульной структурой. Многослойная модульная структура выполняет параллельную обработку запросов от клиентов.

В клиентскую часть модели выполнения лабораторных работ включены функции контроля порядка выполнения работ и контроля полученных результатов моделирования. После выполнения лабораторной работы проводится анализ результатов, выявляются ошибки, даются рекомендации (повторить или перейти к следующей работе). Лабораторная работа засчитывается, если за установленное время были получены правильные результаты. Результаты лабораторных работ формируются в клиентской части и затем передаются на сервер, где они хранятся в ассоциативной памяти.

Достоинством разработанной системы дистанционного обучения является возможность поэтапного обучения и пошагового выполнения лабораторных работ с возвратом к предыдущему и переходом к следующему этапу. Это способствует усвоению и закреплению материала. Многослойная модульная структура модели лабораторных работ позволяет многократно повторять ее для одних и тех же или разных схем оборудования, что не всегда возможно в условиях обычной учебной лаборатории.

Устройство контроля знаний на базе ИНС. Для контроля знаний студента используется ИНС, где хранятся контрольные вопросы, тестовые задачи, а также варианты правильных ответов на естественном и понятном для человека языке [6]. Все контрольные или тестовые задачи разделены по темам. При выполнении контроля знаний студент выбирает тему из числа уже изученных, а вопрос выбирает система обучения случайным образом. ИНС определяет степень соответствия ответа пользователя эталону. После выполнения контроля знаний в базу данных на сервере заносятся оценки, которые студент может потом просмотреть. При неправильном ответе студенту предлагается прочитать анализ его ответа и материал из лекции по данной теме.

Средства редактирования учебно-методических материалов. При создании системы дистанционного обучения важным требованием является простота создания, обновления, дополнения и изменения материалов учебного курса. Для этого предназначен блок редактирования учебно-методических материалов. Этот блок позволяет преподавателям создавать, удалять, изменять материалы к лекциям, практическим занятиям, лабораторным работам, контрольные вопросы и тесты. Для редактирования учебно-методических материалов используется специфика ИНС и возможность ее дополнительного обучения. Добавление учебно-методических материалов приводит к наращиванию слоев в ИНС. Изменение порядка изучения этих материалов приводит к изменению связей между фрагментами ИНС. Изменение содержания одного или нескольких разделов учебно-методических материалов требует переобучения фрагмента ранее обученной ИНС.

Итак, были получены следующие новые результаты:

1. Сформулированы требования к системе дистанционного обучения.
2. Разработана архитектура системы дистанционного обучения на базе ИНС.
3. Разработан новый метод идентификации, аутентификации пользователей и криптографической защиты информации.
4. Разработан комплекс моделей для лабораторных работ на базе ИНС.
5. Разработано устройство для контроля знаний на базе ИНС.

Полученные результаты позволяют реализовать систему дистанционного обучения в технических вузах.

СПИСОК ЛИТЕРАТУРЫ

1. Кабак, И.С. Компьютерные и промышленные сети: учеб. для вузов / И.С.Кабак. – М.: Станкин, 2010. - 275 с.
2. Кабак, И.С. Аппаратная реализация ассоциативной памяти произвольного размера / И.С.Кабак, Н.В.Суханова // Вестник МГТУ «Станкин». - 2010. - № 1. - С. 135-139.
3. Нейронная сеть: пат. на полез. модель № 66831/ Кабак И.С., Суханова Н.В. – Бюл. изобрет. и полез. моделей; приоритет 02.04.07. – 3 с.
4. Доменная нейронная сеть: пат. на полез. модель № 72084 / Кабак И.С, Суханова Н.В. - Бюл. изобрет. и полез. моделей; приоритет 03.12.07. -3 с.
5. Ассоциативная память: пат. на полез. модель №77483 / Кабак И.С., Суханова Н.В. - Бюл. изобрет. и полез. моделей; приоритет 24.12.07. -3с.
6. Устройство контроля знаний: пат. на полез. модель №80979 / Кабак И.С., Суханова Н.В. - Бюл. изобрет. и полез. моделей; приоритет 28.12.07. - 3с.
7. Модульная вычислительная система: пат. на полез. модель № 75247 / Кабак И.С., Суханова Н.В. - Бюл. изобрет. и полез. моделей; приоритет 26.12.08. – 5 с.
8. Многослойная модульная вычислительная система: пат. на изобрет. №2398281 / Соломенцев Ю.М., Шептунов С.А., Кабак И.С., Суханова Н.В. - Бюл. изобрет. и полез. моделей; приоритет 07.11.08. – 5 с.
9. Способ формирования переменного ключа для блочного шифрования данных: пат. на изобрет. №24593367 / Кабак И.С., Суханова Н.В., Позднеев Б.Н. - Оpubл. 20.08.12; приоритет 16.07.10.
10. Способ блочного шифрования сообщений и передачи шифрованных данных с закрытым ключом: пат. на изобрет. №2481715 / Кабак И.С., Суханова Н.В., Позднеев Б.Н. - Оpubл. 05.10.13, Бюл. изобрет. и полез. моделей № 13. - 5с.

Материал поступил в редколлегию 10.07.15.