

матрицы, где методом ГЭО отображаются связи между проектными продуктами (табл. 3).

Затем также при помощи экспертов выделяются группы продуктов и распределяются по 3 формам (малые, средние, крупные). Так формируется логическая структура по внешним связям.

Таблица 3. Логическая структура

1-я зона	2-я зона		3-я зона
Проектный продукт 1	1	■	
Проектный продукт 2		2	■
Проектный продукт 3			3
Проектный продукт 4			4

■ Наличие связи

□ Отсутствие связи

3. *Хроноструктура* характеризуется параметром *время*, под которым понимаем среднестатистическое время, необходимое для достижения результата (создания проектного продукта). Существующие классификации разделяют проекты по продолжительности на мини-проекты, краткосрочные и долгосрочные. Исходя из этого становится возможным конструировать хроноструктуру по периодам: I – до 4 часов; II – до 16 часов; III – до 64 часов. При затрате на создание проекта менее 4 часов невозможно качественное достижение личностного результата.

Такое структурирование элементов воспитательного проекта позволяет внедрить в практику учителя инструмент для построения индивидуального воспитательного маршрута конкретного ученика, действующий в любом направлении воспитательной деятельности по алгоритму:

1) диагностика педагогом начального значения личностных результатов (элементы знаний, отношений и опыта) конкретного обучающегося;

2) подбор педагогом проектных заданий, соответствующих планируемому уровню личностных результатов;

3) разработка и реализация обучающимся на основе этих заданий в течение заданного времени цикла воспитательных проектов с условием продвижения от малой формы проектного продукта к крупной;

4) диагностика промежуточных и конечных личностных результатов.

Включенность экспертов в отбор элементов обеспечивает достоверность результатов структурирования. При условии необходимого организационного и диагностического сопровождения предложенная система структурирования элементов воспитательного проекта позволит педагогу достичь запланированных личностных результатов и развития тезауруса конкретного обучающегося.

Библиографические ссылки

1. Концепция Федеральной целевой программы развития образования на 2016–2020 годы.
2. *Караковский В. А.* Статья человеком // Воспитательная работа в школе. – 2015. – № 2. – С. 10–46.
3. *Сергеев И. С.* Как организовать проектную деятельность учащихся : Практическое пособие для работников общеобразовательных учреждений. – 7-е изд., испр. и доп. – М. : АРКТИ, 2009. – 80 с.
4. *Мирошниченко А. А., Куртеева О. В.* Квалиметрия воспитательного проекта // Вестник ИжГТУ. – Ижевск, 2014. – № 2(62). – С. 182–184.
5. *Мирошниченко А. А.* Теория и технология конструирования профессионально ориентированных структур учебных элементов : дис. ... д-ра пед. наук. – Глазов, 1999.
6. Там же.
7. *Беспалько В. П.* Слагаемые педагогической технологии. – М., 1989. – 190 с.
8. *Мирошниченко А. А., Куртеева О. В.* Указ. соч.
9. *Мирошниченко А. А.* Указ. соч.
10. Там же.
11. *Титова Е. В.* Если знать, как действовать : Разговор о методике воспитания : Кн. для учителя. – М. : Просвещение, 1993. – 192 с.

Получено 30.06.2016

УДК 004.421:378

В. Н. Емельянов, кандидат технических наук, ИжГТУ имени М. Т. Калашникова
М. М. Емельянова, ИжГТУ имени М. Т. Калашникова
Р. В. Пушин, магистрант, ИжГТУ имени М. Т. Калашникова

АЛГОРИТМ ПРОВЕРКИ ПОДЛИННОСТИ ПОЛЬЗОВАТЕЛЕЙ В СИСТЕМЕ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

Главной целью любого образовательного процесса является получение студентами необходимого количества знаний и навыков, степень усвоения которых определяется результатами различных контрольных и самостоятельных заданий. При стандартной форме обучения не возникает осо-

рых сложностей проверки качества знаний обучающихся, так как у преподавателя есть возможность контролировать весь процесс аудиторных занятий [1, 2]. При дистанционной форме обучения проблема проверки качества знаний является актуальной. Это обусловлено тем, что между пользователем и препо-

давателем нет прямого контакта и уверенности в том, что задание выполняет сам студент. Таким образом, основная задача системы дистанционного обучения (ДО) при оценке знаний – обеспечение полноценной проверки подлинности (аутентификации) удаленного пользователя.

В настоящее время существуют высокотехнологичные программно-аппаратные средства верификации различных биометрических параметров человека, например, сканирование сетчатки глаза, отпечатка пальца, ладони, распознавание пользователя по голосу. Но данные технологии имеют существенные недостатки – сложность реализации и высокая стоимость оборудования. В настоящее время такие технологии невозможно внедрить в большинстве систем дистанционного обучения.

На практике достаточно часто применяются два других метода.

Один из технологичных и относительно низкозатратных методов аутентификации – технология распознавания лиц. Для реализации данного метода достаточно веб-камеры пользовательского устройства и специального программного обеспечения. Существует несколько алгоритмов аутентификации пользователей: метод гибкого сравнения на графах, нейронные сети, скрытые марковские модели, метод главных компонент. Но процесс распознавания лиц происходит по общей схеме: сканирование, сравнение и распознавание [3, 4]. Данный метод имеет следующие недостатки: сложность процедуры, которая заключается в том, что аутентификация пользователя происходит посредством сравнения изображения лица с заложенным эталоном. Изменение освещения, угол съемки, изменение мимики – все это влияет на правильность работы системы.

Следующий метод – аутентификация пользователя по клавиатурному почерку. Как и в любой системе аутентификации здесь необходимо создать некий шаблон, с которым будет сравниваться идентификатор пользователя, в данном случае – стиль работы на клавиатуре. Для корректной работы системы необходимо провести ее обучение, в результате чего происходит обработка первичных данных, из которых выделяются эталонные признаки работы пользователя с клавиатурой.

Для обучения системы пользователю необходимо некоторое число раз напечатать предлагаемый текст, на основании которого будет собираться и обрабатываться информация о работе пользователя с клавиатурой, в базе сохраняются эталонные характеристики.

Наиболее постоянным и точным параметром клавиатурного почерка являются подсознательные процессы мышления. Размер и сложность фразы, опыт работы, навыки пользования клавиатурой значительно влияют на процесс аутентификации. Таким образом, для точной аутентификации методом клавиатурного почерка необходимо учитывать сознательные и подсознательные процессы мышления, использовать несложные фразы и учитывать опыт работы пользователя [5].

Данный метод подойдет для проверки подлинности пользователя при выполнении заданий, где необходимо давать развернутые ответы; для проведения тестирования данный метод неуместен. С течением времени клавиатурный почерк человека изменяется, следовательно, система аутентификации требует периодического переобучения.

Алгоритм проверки подлинности пользователя в системе ДО

Для проверки подлинности пользователя во время тестирования авторами разработан и предлагается к использованию метод случайного опроса, который состоит из двух этапов.

Первый этап – присвоение пользователю логина и пароля, базовое действие в любой электронной системе.

Второй этап – заполнение анкеты пользователем. Анкета должна содержать вопросы и информацию о пользователе, которая известна только ему и достаточно проста для запоминания, например, дата рождения, имя, фамилия, также может содержаться информация о близких родственниках. Вопросы о любимой еде, цвете, музыке в данном случае будут неуместны, так как ответы на них зависят от многих факторов и могут часто меняться. Ниже будут приведены примеры используемых вопросов.

В разработанной системе предполагается использование так называемого фактора внезапности, путем постановки неожиданных («любовых») вопросов в ситуации, когда студент таких вопросов не ждет, успокоенный «безопасным», с его точки зрения, содержанием и направлением выполнения задания. Это работает в том случае, если системой пользуется постороннее лицо, не ожидающее появления личных вопросов. Вопросы будут складываться из информации заполненной анкеты.

Выполнение предлагаемой процедуры проверки подлинности пользователя приведено в блок-схеме, представленной на рисунке.

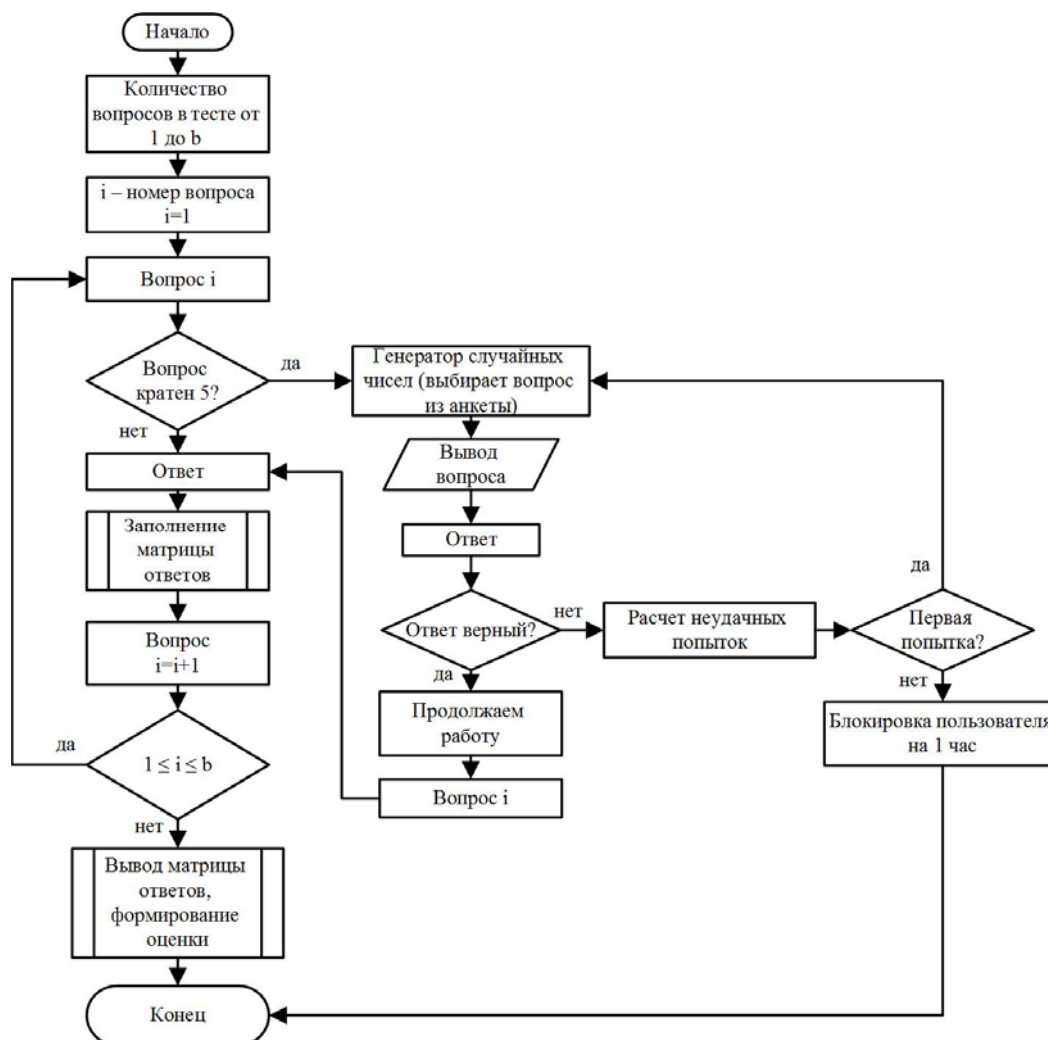
Во время выполнения задания в произвольном порядке периодически студенту будут задаваться вопросы из списка анкеты. Время для ответа будет ограничено (например, около 10 с), это делается для того, чтобы нелегитимный пользователь не успел получить необходимую информацию. Если ответ верный, пользователь проходит аутентификацию и продолжает работу, если нет – ему дается вторая попытка. При повторной неудаче тест блокируется для пользователя на определенное время (например, 1 час), после чего для входа в систему необходимо снова пройти процедуру аутентификации.

При вводе ключевого слова не исключена вероятность появления ошибки, например, опечатки. Чтобы свести к минимуму отказ в доступе при опечатке, система должна допускать появление некоторой ошибки, не превышающей определенного порога, например, 1 символ на слово или фразу. Также необходимо учитывать длину ключевого слова, так как чем короче ключ, тем меньше ошибок в нем можно

допустить. Также недопустимы опечатки в ответах, требующих ввода цифровых значений.

Данный метод позволит контролировать пользователей системы дистанционного тестирования и повысить качество проверки знаний пользователей. Для данного метода очень важным становится опре-

деление корректных вопросов анкеты и вероятностей ошибки истинного пользователя при повторном ответе на них. Однажды заполнив тестовую анкету, учащийся может просто забыть собственный ответ на задававшийся вопрос. Важно выявить реальную оценочную величину такой вероятности.



Блок-схема процедуры проверки подлинности пользователя

Опыт реализации алгоритма проверки подлинности

Для решения поставленной задачи были проведены следующие эксперименты. Проведена регистрация и анкетирование учащихся ИжГТУ имени М. Т. Калашникова в системе тестирования MOODLE. Были опрошены три группы учащихся: бакалавры очного отделения кафедры «Сети связи и телекоммуникационные системы» (16 человек), заочного отделения кафедры «Сети связи и телекоммуникационные системы» (20 человек) и инженеры, проходящие курсы повышения квалификации (14 человек).

В анкете было использовано 15 вопросов, представленных в таблице.

Студентам разрешалось не отвечать на вопросы, которые они по некоторым причинам считают неуместными. На каждый вопрос давалось 10 секунд.

Через 14 дней было проведено повторное электронное тестирование в системе MOODLE с использованием ранее указанных вопросов, после чего были подсчитаны ошибки и их частота при повторном ответе на указанные вопросы.

Результаты ответов сведены в таблицу. $P_{\text{ош.1}}$, $P_{\text{ош.2}}$, $P_{\text{ош.3}}$, $P_{\text{ош.}}$ – подсчитанные по анкетам частоты (вероятности) ошибок при повторном ответе на вопрос для учащихся заочного отделения, инженеров, проходящих курсы повышения квалификации, бакалавров очного отделения и общая вероятность по всем тестируемым соответственно.

Как видно из приведенных результатов, учащиеся практически не ошибаются при ответах на вопросы, требующие однозначного и простого ответа (например, вопросы 4, 7–11). В то же время если ответ на такой вопрос требует изложение конфиденциальной, персональной информации (как в вопросах 2, 5 и 6),

то некоторые из учащихся могут давать выдуманный ответ, который забывают при повторении такого же вопроса. Но если использовать такие простые вопро-

сы в процедуре проверки подлинности, то очень просто обмануть данный алгоритм, так как легко запомнить односложные ответы.

Частоты неправильных повторных ответов

Вопросы анкеты	$P_{\text{ош.1}}$	$P_{\text{ош.2}}$	$P_{\text{ош.3}}$	$P_{\text{ош.}}$
1. Год рождения одного из родителей	0,22	0,29	0,25	0,25
2. Дата рождения пользователя (день, месяц год, написать без пробела)	0	0,29	0	0,08
3. Год окончания средней школы	0,2	0,29	0	0,16
4. Место рождения (название населенного пункта)	0	0,14	0	0,04
5. Последние 4 цифры номера телефона	0,1	0,14	0	0,08
6. Номер дома	0,1	0,17	0,13	0,13
7. Название улицы, где вы проживаете	0,1	0	0	0,04
8. Месяц вашего рождения (слово)	0	0	0,13	0,04
9. Ваш знак зодиака	0	0	0	0
10. Девичья фамилия матери	0	0	0	0
11. Номер школы, в которой вы учились	0	0	0	0
12. Просуммируйте номер вашего дома и квартиры	0,22	0,33	0,13	0,22
13. Вычтите 10 из числа, которое получается из двух последних цифр номера телефона одного из ваших родителей	0,57	0,83	1	0,73
14. Умножьте последнее число вашего номера телефона на номер дома	0,25	0,5	0,14	0,29
15. ФИО отца без расшифровки и день его рождения (написать без пробелов, например, ПВН06)	0,3	0,33	0	0,21

Тестируемые чаще ошибались при вводе ответов на вопросы, ответ на который они первоначально могли не знать или забыть (вопросы 1 и 3). Также частота ошибок велика при ответах на вопросы, требующих выполнения некоторой операции (как в вопросах 12–15), например, сложения, но вероятность ошибки не критична (как показал расчет доверительного интервала для математического ожидания нормального распределения случайной величины, верхняя граница составляет около 26 %). При использовании таких вопросов необходимо аккуратно отнестись к формулировкам, избегая неоднозначности, которая присутствует в вопросах 1, 13, 14.

Именно подобные вопросы с возможностью неоднозначных ответов необходимо использовать для реализации системы проверки подлинности удаленного пользователя, закладывая максимальную вероятность ошибки 0,26.

В будущем планируется исследовать оптимальность значений вероятности ошибки пользователя при ответе на вопросы анкеты, при разных длинах ответа и типах вопросов.

Получено 04.07.2016

Библиографические ссылки

1. Емельянов В. Н., Павлова М. М. Методика оценки выполнения заданий в электронных системах обучения // Вестник ИжГТУ имени М. Т. Калашникова. – 2015. – № 3(67). – С. 138–140.
2. Emelianov V., Emelianova M. Method of performance evaluation of tasks in elearning // Сборник статей I Международ. форума ИЕЕТ-2015, проводимого в рамках XI Международ. науч.-техн. конф. «Приборостроение в XXI веке. Интеграция науки, образования и производства». – Ижевск : Изд-во ИжГТУ имени М. Т. Калашникова, 2016. – С. 64–68.
3. Wansen Wang, Hui Fang Niu. Face detection based on improved AdaBoost algorithm in E-Learning // 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems (CCIS), 2012.
4. Stankov S. Intelligent Tutoring Systems in E-Learning Environments: Design, Implementation and Evaluation. – IGI Global, 2010. – 446 p.
5. Технология усиленной аутентификации пользователей информационных процессов / И. А. Холашинский, М. В. Савчук, И. В. Горбунов, Р. В. Мещеряков // Доклады Томского гос. ун-та систем управления и радиоэлектроники. – Томск : ТГУСУиР, 2011. – № 3. – С. 236–248.