

## ПОСТАНОВКА ЗАДАЧИ ПО РЕАЛИЗАЦИИ ДОВЕРЕННОГО СЕАНСА СВЯЗИ ПРИ ДИСТАНЦИОННОМ ОБУЧЕНИИ<sup>1</sup>

Фундаментальной проблемой высшего образования является формирование у обучающихся устойчивых навыков самостоятельного и своевременного получения определенной суммы знаний, построения исследовательских гипотез и критической оценки полученных результатов. Очевидным способом ее решения является эффективное использование таких технологий обучения, при котором реализуется активное взаимодействие обучаемого с преподавателями и коллегами, взаимный обмен мнениями и опытом решения той или иной задачи.

Также очевидно, что используемые в настоящее время системы дистанционного обучения не дают должного эффекта в этом плане, так как они во многом основываются на традиционной подаче «архивных» материалов при отсутствии интерактивного взаимодействия преподавателя и обучаемого, то есть сам обучаемый, как правило, не участвует в формировании, а лишь является пассивным участником учебного процесса.

Так, известные разработки, в частности технологии E-learning (обучение через персональные компьютеры), M-learning (обучение через мобильные телефоны и переадресация на ПК), I-learning (интерактивное обучение), не обеспечивают необходимого уровня доверия к процедуре проверки знаний. А E-learning-решения к тому же не предлагают доступных и качественных способов контроля обучения конкретного слушателя. Это снижает доверие к качеству обучения, которое в существующих системах может быть обеспечено пока лишь при введении дополнительных очных процедур контроля знаний.

Суть поставленной проблемы хорошо иллюстрируется скандалами с процедурами приема ЕГЭ, широко освещаемыми в средствах массовой информации.

Поэтому не будет преувеличением вывод о том, что в настоящий момент отсутствие доступных и достоверных способов аутентификации (подтверждения подлинности) обучаемого в процессе обучения, а главное, в ходе дистанционного контроля знаний не дает полноценного уровня доверия к применению дистанционной системы тестирования в ходе промежуточного и итогового контроля знаний [1].

То есть на данный момент весьма актуально найти такой нетрадиционный путь подачи учебного материала, опирающийся на новые информационные технологии, чтобы:

- 1) у обучаемого появилась реальная возможность самостоятельного или совместного с преподавателем формирования своего учебного процесса в режиме реального времени;
- 2) был обеспечен гарантированный уровень доверия к результатам обучения.

Реализация поставленной задачи, на наш взгляд, возможна при внедрении в процедуры дистанционного обучения перспективных информационных технологий видеоконференцсвязи (ВКС) с использованием доверенной среды связи (ДСС).

Видеоконференцсвязь — это средство совместной работы территориально удаленных пользователей или групп пользователей или сеанс связи в режиме реального времени между географически удаленными пользователями.

В настоящее время на рынке присутствуют два подхода в реализации видеосвязи:  
- системы с выделенным оконечным оборудованием (от настольных систем до систем для переговорных комнат), такие как: Tandberg, Polycom и др.;

<sup>1</sup> Данная работа выполнена в НИЯУ МИФИ при финансовой поддержке Министерства образования и науки Российской Федерации в рамках проекта «Создание научно-методических основ единой образовательной информационно-телекоммуникационной среды в области информационной безопасности».

- системы, основанные на программных решениях с использованием ПК, такие как: Skype, MS Messenger, Yahoo Messenger и др.

Главное достоинство ВКС с точки зрения дистанционного обучения состоит в том, что обучаемый легко в режиме реального времени получает информацию непосредственно от специалиста в предметной области, следит за динамикой ее изменений непосредственно на производственном объекте обучения (исследований). А у преподавателя есть уверенность в том, что его действительно слушают и правильно интерпретируют его слова.

Как известно, неформальным определением термина «доверие» применительно к аппаратным средствам и ИТ-продуктам является наличие основы для уверенности в том, что ИТ-система отвечает всем требованиям безопасности [2]. Поэтому суть концепции ДСС состоит в том, что необходимый уровень защищенности ИТ-системы обеспечивается не в течение всего времени ее эксплуатации, а только в те периоды времени, когда высокая защищенность действительно необходима.

Одним из действующих программно-аппаратных комплексов, решающим такую задачу создания доверенной среды функционирования, является комплекс СОДС «МАРШ!» [3, 4, 5].

СОДС «МАРШ!» как средство обеспечения доверенного сеанса связи предполагает:

- полноценную криптографическую защиту;
- возможность работы на любом компьютере в обычном режиме и в режиме ДСС;
- приемлемые стоимость и затраты в процессе эксплуатации;
- простоту использования, мобильность и компактность.

Реализация ДСС совместно с использованием технологий ВКС, на наш взгляд, даст существенное преимущество, **состоящее в повышении качества подачи и увеличении количества учебного материала в рамках современного дистанционного образовательного процесса, а также в получении** активной, аутентифицированной (!) обратной связи с обучающимися и необходимого уровня доверия к контролю его знаний. Становятся возможными и контроль качества проведения лекций, семинаров и других видов занятий за счет ведения их удаленного просмотра учебно-методическим персоналом с одновременной видеоархивацией; создание банка (библиотеки) видеолекций и видеовыступлений известных специалистов и ученых и их рассылка по запросу; использование фотоидентификации преподавателей и студентов с целью контроля посещаемости и исключения случаев фальсификации результатов различного рода испытаний и экзаменов; появляется реальная возможность интеграции технологий ВКС в существующую систему безопасности образовательного учреждения и др.

## СПИСОК ЛИТЕРАТУРЫ:

1. Алюшин В. М., Горбатов В. С., Дураковский А. П., Милославская Н. Г., Петров В. Р., Толстой А. И. О необходимости шифрования в системах дистанционного обучения // Материалы Международной конференции ТОП-2013. УНИАР. URL: <http://www.topro.ru/>
2. Бородакий Ю. В., Добродеев А. Ю., Бутусов И. В. Доверенная среда — основа гарантированной безопасности! // Information Security / Информационная безопасность. 2013. № 2. С. 36–37.
3. Чугринов А. В. Доверенные сеансы связи и средства их обеспечения // Information Security / Информационная безопасность. 2010. № 4. С. 54–55.
4. Конявская С. В. Безопасность Web-ресурса. Иллюзии с последующим разоблачением // Information Security / Информационная безопасность. 2011. № 2. С. 53.
5. Конявская С. В. Шашечки или ехать? Всегда ли безопасность обеспечивается именно защищенностью? // Information Security / Информационная безопасность. 2012. № 4. С. 42–43.

