Проблема доверия при организации новых форм обучения на основе интернет-технологий

Анатолий Дураковский, Виктор Горбатов, Владислав Петров
Национальный исследовательский ядерный институт «МИФИ», Россия
APDurakovskiy@mephi.ru, VSGorbatov@mephi.ru, VRPetrov@mephi.ru

Одним из приоритетных направлений развития сферы образовательных услуг является ориентация на массовые формы обучения, среди которых отечественное законодательство выделяет дистанционное (электронное) образование и сетевую реализацию образовательных программ [1]. Материально - технической основой таких форм обучения являются интернет-технологии, широко представленные на рынке IT-продукции и активно внедряемые образовательными учреждениями в практику своей деятельности.

С учетом технологических достижений на первый план, на наш взгляд, выходит решение так называемой проблемы доверия, не имеющей к настоящему времени общепринятого определения. О том, что такая проблема существует, свидетельствует, по крайней мере, опыт внедрения в практику отечественной образовательной системы аттестации в форме ЕГЭ.

Настоящая работа посвящена формулированию указанной проблемы и определению подходов по ее решению.

Возникновение проблемы доверия при использовании указанных выше новых форм обучения связано с необходимостью выполнения требований действующих нормативных правовых актов, в соответствии с которыми образовательные учреждения вправе применять электронное обучение, дистанционные образовательные технологии при проведении учебных занятий, практик, текущего контроля успеваемости, промежуточной, итоговой и (или) государственной итоговой аттестации обучающихся. Но при этом на образовательное учреждение возлагается обязанность по ведению учета и хранения результатов образовательного процесса, а также внутреннего документооборота, в том числе в электронно-цифровой форме в соответствии с принятой политикой информационной безопасности, полностью соответствующей отечественному законодательству [2]. В соответствии с терминологией, установившейся в области обеспечения информационной безопасности, проблему доверия в образовательных интернет - технологиях можно представить как необходимость безусловного выполнения следующих требований:

- доступности информационных ресурсов;
- конфиденциальности [1];

- целостности.

Положение с проблемой доверия в интернет-технологиях усугубляется тем, что в соответствии с работой [3] решения на их основе, в частности дистанционные образовательные технологии, относятся к так называемым открытым системам.

Реализуя на практике российскую программу “Информационное общество (2011-2020)” посредством “облачных вычислений” в ДО по модели SaaS (Software as a Service) встает вопрос «доверия» и защищенности получаемой информации из недоверенной среды.

Стоит отметить, что в настоящее время отсутствуют стандартизированные подходы, регламентирующие процедуры контроля процесса обучения и выполнения всевозможных контрольно-измерительных мероприятий.

Определим открытую доверенную IT – среду как совокупность технических и программных средств, обеспечивающих создание, применение и развитие системы в соответствии с предназначением, и имеющих полный комплект программной, конструкторской и эксплуатационной документации, включая исходные тексты программ, отвечающих необходимым требованиям информационной безопасности, подтвержденных аттестатами соответствия (аудиторскими заключениями) в соответствующих системах технического регулирования.

Анализ ряда источников [4, 5, 6, 7] показал, что использование публичного «облака» как основы дистанционного обучения не является безопасным с точки зрения такого определения «доверия», так как в настоящее время отсутствуют общепринятые требования к системе защиты «облака», детализированная (частная) модель угроз безопасности сред облачных вычислений, которая в настоящее время отсутствует, следовательно, применение облачной инфраструктуры несет за собой повышенные риски и более ограниченные возможности контроля. Это одна из главных проблем облачных вычислений – формирование «доверия» пользователей по отношению к облачным провайдерам, к их возможностям формирования доверенной среды.

Более того, отсутствие регламентированных требований к автоматизированным рабочим местам (АРМ) участников процесса дистанционного обучения, приводит процесс их взаимодействия с образовательным учреждением к объективному «недоверию».

Анализ литературных источников показывает, что в настоящее время ни один из IT-продуктов, предлагаемых на российском рынке обеспечения дистанционного обучения (как «облачные», так и «локальные») не гарантирует необходимый уровень

защищенности при работе в СДО в рамках закона об образовании [1] даже при условии применения отдельных средств защиты информации, т.е. возможны несанкционированные доступы к материалам СДО, атаки на пользователя, на СДО, на преподавателя, подмены пользователя и, как следствие, изменение/оспаривание результатов теста.

В работе сформулирован критерий “Трех доверий” к трем ключевым составляющим процесса ДО:

- АРМ участников процесса, включая систему ДО и доступ к ней;
- к каналу передачи информации между участниками процесса ДО, что позволит внедрить дополнительный параметр подлинности;
- аутентичности участников процесса ДО, в том числе, но не исключая, с использованием биометрических способов.

По мнению авторов реализация данного критерия в дистанционных образовательных технологиях позволит обеспечить выполнение требований и рекомендаций, предъявляемых в основополагающих нормативных актах Российской Федерации [1, 2, 8], регулирующих образовательный процесс с применением средств дистанционного электронного обучения, к обеспечению необходимого уровня информационной безопасности, а так же достоверного подтверждения результатов контрольных измерительных мероприятий и высокой степени подтверждения неотказуемости от сообщений и отправлений путем формирования единой доверенной среды между участниками процесса ДО с использованием аутентификации по биометрическим признакам.

Ссылки

1. Федеральный закон от 29.12.2012 N 273-ФЗ (ред. от 21.07.2014) "Об образовании в Российской Федерации".
2. Приказ Минобрнауки России от 09.01.2014 N 2 "Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ".
3. Кривопалов В.Г. Комплексная методика моделирования рисков информационной безопасности открытых систем, диссертация на соискание ученой степени кандидата технических наук по ВАК 05.13.19, Электронная библиотека диссертаций Российской государственной библиотеки, [Электронный ресурс]. URL: https://dvs.rsl.ru/ (дата обращения: 13.08.2014).

4. Бабанин А.В. Безопасность в облаке: мифы и реальность. Обеспечение безопасности и безопасность как сервис // Information Security / Информационная безопасность. 2013. № 1. С. 34–35.
5. Чирков К.А., Паньчев С.В. Особенности организации защиты информации в информационных системах МВД России с учётом особенностей «облачной архитектуры» // Информационные технологии, связь и защита информации МВД России. 2012. С.30-32. [Электронный ресурс]. URL: http://www.mvd.informost.ru/2012/pdf/part1/1-9.pdf (дата обращения: 09.08.2014).
6. Ивонин П.В. Безопасность облака в деталях // Безопасность информационных технологий 2013. №2. С. 37-40.
7. Безопасность в облаках: над чем нам работать? // CONNECT. 2012. № 7–8. С. 128-134. [Электронный ресурс]. URL: http://www.aladdin-rd.ru/support/downloads/get?ID=35691 (дата обращения: 09.08.2014).
8. ГОСТ Р 54471-2011/ISO/TR 15801:2009. Системы электронного документооборота. Управление документацией. Информация, сохраняемая в электронном виде. Рекомендации по обеспечению достоверности и надежности. [Текст] Введ. 2012-08-01. – М.: Стандартинформ, 2012.