

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ ОБРАЗОВАНИЯ

А.А. Кашкароева, канд. социол. наук, доцент

Н.Э. Атаканова, преподаватель

**Институт социального развития и предпринимательства
(Кыргызстан, г. Бишкек)**

***Аннотация.** Проблемы информационной безопасности в системах открытого образования обсуждаются с точки зрения личности, общества и государства. Рассматриваются потенциальные и реальные угрозы информационной безопасности и объекты, которые нуждаются в защите. Исследуются взгляды студентов и преподавателей на проблемы конфиденциальности информации в компьютерно-ориентированной педагогической среде. Предлагаются подходы к поиску путей предупреждения и преодоления угроз информационной безопасности.*

***Ключевые слова:** информационная безопасность, информационно-коммуникационные технологии, информационный продукт, информационные угрозы.*

Постановка проблемы. Системы открытого образования создают перспективный базис развитию педагогической среды для обучения на протяжении всей жизни - одного из приоритетных направлений программы ЮНЕСКО «Информация для всех». Проблемы повышения эффективности открытого образования, исследования моделей его организационных форм [1], совершенствования методов и способов обучения находятся в центре внимания исследователей. В основе открытого образования - широкое применение информационно-коммуникационных технологий для поддержки учебного процесса, его личностной ориентации, повышения комфорта и эффективности учебной деятельности, что «...порождает критическую массу новых задач, решение которых невозможно без создания прочного междисциплинарного научного базиса, который гибко сочетает в себе классические научные решения и результаты их практической реализации» [2]. Как и в любой сложной системе, которая играет весомую роль в развитии потенциала каждого отдельного государства и общества в целом, предполагает массовое привлечение специалистов и использование информационно-коммуникационных технологий, в системе открытого образования следует уделить внимание вопросам информационной безопасности, проанализиро-

вать возможные угрозы и пути защиты от них.

Анализ последних исследований и публикаций. Информационную безопасность в системах образования следует рассматривать в контексте общих вопросов безопасности информационных систем с опорой на соответствующие законодательные акты. Так в доктрине информационной безопасности Кыргызстана [3] выделено жизненно важные интересы личности, общества и государства, а также реальные и потенциальные угрозы информационной безопасности. Проблемы комплексной защиты информационных систем активно прорабатываются зарубежными и отечественными специалистами [4]. К вопросам информационной безопасности систем открытого образования относятся исследования безопасности личности в сети Интернет, в частности, защита от разнообразных технологий мошенничества и защита от материалов, которые нежелательны с точки зрения общественной морали и нормального развития человека. Исследователи анализируют процесс развития новых информационных технологий и считают, что наступило время контролируемого приспособления коммуникативной реальности к образовательной практике [5]. Первоочередное внимание уделяется информационной безопасности в общеобразовательных учебных заведениях на основе внедрения комплекса технических,

административных и воспитательных мероприятий и предлагается функциональная модель обеспечения информационной безопасности старшеклассника в компьютерно-ориентированной учебной среде. Обращается внимание на необходимость формирования компетентности в области информационной безопасности. Большое значение уделяется проблемам борьбы и сотрудничества в информационной сфере, которые, на наш взгляд, распространяются и на сферу образовательных услуг, и на научные исследования. Проблемы информационной безопасности дистанционного взаимодействия субъектов учебного процесса рассматриваются и в контексте психологической безопасности личности. Выделение нерешенных ранее частей общей проблемы. Как видим, проблемы защиты информации в технических компонентах системы открытого образования очерчены в современных исследованиях, однако вопросы безопасности в процессах взаимодействия человека с информационной средой во время учебной деятельности требуют глубокого изучения, что и определяет актуальность данного исследования.

Цель данной статьи - описание комплексной системы угроз информационной безопасности личности и общества в системах открытого образования.

Потенциальные угрозы информационной безопасности основных объектов в системе открытого образования

Выделим основные информационные объекты в системе открытого образования, которые нуждаются в защите:

учебные материалы, созданные авторами курса и размещенные в сети;

материалы, создаваемые коллективно участниками учебного процесса;

персональные данные, результаты педагогической диагностики и мониторинга учебных достижений обучаемых, хранящиеся в информационной системе на одном или нескольких серверах;

информация о деятельности участников учебного процесса, которая осуществляется с использованием определенных общедоступных сервисов Интернет. Информационные угрозы относительно учебных материалов и других данных, размещенных в сети, не отли-

чаются от подобных угроз в любой информационной системе. В первую очередь, это случайные угрозы, связанные с ошибками персонала или разработчиков, отказами технических средств, авариями и влиянием внешних факторов. Умышленное нарушение целостности информации, несанкционированный доступ к ней, умышленное препятствование доступу пользователей к информации или повреждение информационной системы не характерно для образовательных систем, но иногда акты вандализма имеют место и соответствующие механизмы должны быть предусмотрены в системе защиты. Однако традиционные меры комплексной защиты информации будут вполне эффективны в системе открытого образования для всех ее компонентов, размещенных в сети.

Иная ситуация возникает, когда речь идет про ресурсы, создаваемые коллективно. Дополнительно к традиционным информационным угрозам следует учитывать ошибки пользователей, не имеющих достаточной готовности к самоанализу качества собственных информационных продуктов. Информационный продукт со значительным количеством ошибок представляет опасность для других участников учебного процесса. Даже человек с высоким уровнем критического мышления и предметной подготовки не всегда готов заметить ошибку в приведенных фактах или искривление значимости тех или иных аспектов проблемы. Ошибка в учебных материалах усваивается на уровне подсознания и приводит к подмене информации на уровне учебных достижений обучаемого. Более того, когда состав учебных групп не однородный по социально-этическим взглядам, возможно навязывание определенных идей той частью группы, которая многочисленнее или более активна. Никакие технические средства не снижают указанную информационную угрозу. Ее преодоление требует реализации комплекса организационных и воспитательных мероприятий, обеспечения определенного уровня подготовки пользователей коллективных систем создания учебной информации. Значительная

роль в обеспечении качества коллективного информационного продукта принадлежит преподавателю-модератору, целесообразно создавать экспертные группы из наиболее подготовленных студентов, важно развивать у обучаемых навыки самоанализа и критического мышления, уважение к мнению коллег.

Безопасность персональных данных

Проблема безопасности персональных данных в значительной степени определяется уровнем открытости таких данных и морально-этическими взглядами в конкретной социальной среде. Поэтому, чтобы определить круг субъектов, которым обучаемые доверяют свои персональные данные про ход и результаты учебной деятельности, был проведен опрос среди преподавателей и студентов университетов. Анкета включала вопросы для определения содержания информации о ходе учебного процесса, которая подлежит защите, и определения круга субъектов, которым эта информация должна быть доступна. Общее число респондентов, которые высказали свое мнение по вопросам анкеты, составило 159 человек, соотношение мужчин и женщин - 1:2 как среди преподавателей, так и среди студентов.

На рассмотрение участников опроса было предложено пять ситуаций взаимодействия студента с информационно-коммуникационной педагогической средой, в которых возможно накопление информации об учебной деятельности с целью педагогической диагностики и управления учебным процессом:

ситуация 1 - в рамках педагогического контроля преподаватель проводит тестирование учебных достижений. Анализ тестовых результатов позволяет исследовать уровень и структуру учебных достижений студента;

ситуация 2 - в процессе самостоятельной работы студент пользуется автоматизированной системой тестирования учебных достижений. Анализ тестовых результатов позволяет исследовать уровень и структуру учебных достижений студента;

ситуация 3 - в ходе занятия проводится видеозапись аудитории. Анализ видеозаписей можно использовать для изучения индивидуального поведения и психологических характеристик студента;

ситуация 4 - во время работы студента с компьютерными программами учебного назначения осуществляется регистрация последовательности его действий, времени, качества выполнения заданий, обращений к справочной информации, выбора внешнего вида экрана, настроек меню, особенностей использования клавиатуры и мыши и т. д. Анализ таких данных позволяет получить информацию о психологических и физиологических особенностях студента, а также об уровне и структуре учебных достижений;

ситуация 5 - во время работы студента за компьютером с помощью видеокамеры и специальных датчиков осуществляется регистрация его физиологических параметров, например таких, как подвижность, частота пульса, кардиограмма и т. д. Анализ таких данных позволяет получить информацию о состоянии здоровья студента и уровень его утомления. Этими данными можно воспользоваться для выработки рекомендаций студенту относительно оптимального для него режима труда и отдыха.

Следует ли вообще защищать информацию о ходе учебного процесса от несанкционированного доступа? Ответы респондентов (рис. 1) показывают, что число сторонников конфиденциальности и открытости таких данных близка. Значительная часть респондентов считает, что такие данные не могут быть использованы во вред преподавателю или студенту, что свидетельствует о высоком уровне взаимного доверия в обществе. Однако, учитывая мнения другой половины респондентов, доступ участников учебного процесса к персональным данным относительно учебной деятельности должен быть регламентирован.

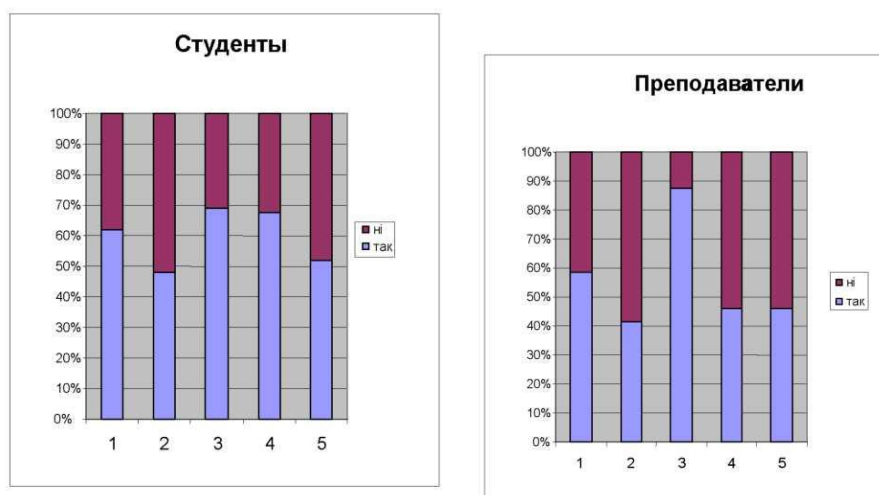


Рис. 1. Распределение ответов преподавателей и студентов на вопрос анкеты «Понимаете ли Вы, что эти данные могут быть использованы во вред студенту или преподавателю?» соответственно ситуациям:

- 1 - ситуация 1, 2 - ситуация 2,
3 - ситуация 3, 4 - ситуация 4,
5 - ситуация 5.

Анализ ответов студентов и преподавателей отдельно по каждой ситуации свидетельствует о том, что наиболее конфиденциальной люди старшего поколения (преподаватели) считают видеозапись во время занятий (87% респондентов, 95%-й доверительный интервал составляет $\pm 14\%$). Студенты признают наиболее конфиденциальными видеозапись аудитории (ситуация 3) и фиксацию их деятельности во время работы за компьютером (ситуация 4) (69% и 68% респондентов соответственно, доверительный интервал $\pm 9\%$). По другим ситуациям существенных расхождений в ответах студентов и

преподавателей не наблюдается.

Исследование взглядов студентов и преподавателей на круг субъектов, которым следует иметь доступ к информации о ходе учебного процесса (табл. 1 и табл. 2) показывает, что большинство участников учебного процесса полностью доверяют свои персональные данные только преподавателю данной конкретной дисциплины.

Таблица 1

Частота ответов преподавателей на вопрос анкеты «Кто, по вашему мнению, должен иметь доступ до диагностических данных?»

Таблица 2

| Субъект учебного процесса | Информационная ситуация | | | | |
|-------------------------------|-------------------------|------------|------------|------------|------------|
| | Ситуация 1 | Ситуация 2 | Ситуация 3 | Ситуация 4 | Ситуация 5 |
| преподаватель | 79% | 38% | 75% | 75% | 54% |
| психолог | 42% | 29% | 63% | 54% | 58% |
| куратор | 46% | 25% | 46% | 25% | 29% |
| родители | 42% | 13% | 13% | 21% | 42% |
| декан | 25% | 8% | 17% | 13% | 25% |
| весь коллектив преподавателей | 25% | 17% | 8% | 8% | 17% |
| другие студенты группы | 8% | 8% | 4% | 4% | 0% |

Частота ответов студентов на вопрос анкеты «Кто, по вашему мнению, дол-

жен иметь доступ до диагностических данных?»

Таблица 3.

| Субъект учебного процесса | Информационная ситуация | | | | |
|-------------------------------|-------------------------|------------|------------|------------|------------|
| | Ситуация 1 | Ситуация 2 | Ситуация 3 | Ситуация 4 | Ситуация 5 |
| Преподаватель | 82% | 52% | 72% | 77% | 65% |
| Психолог | 33% | 14% | 50% | 39% | 53% |
| Куратор | 20% | 9% | 31% | 29% | 34% |
| Родители | 24% | 9% | 16% | 12% | 28% |
| Декан | 13% | 3% | 17% | 13% | 16% |
| Весь коллектив преподавателей | 8% | 3% | 13% | 14% | 19% |
| Другие студенты группы | 13% | 3% | 17% | 13% | 2% |

Таким образом, необходимо обеспечить конфиденциальность персональных данных участников учебного процесса не только по отношению к внешним «злоумышленникам», но и внутри организации, предоставляющей образовательные услуги. Угроза нецелевого использования результатов педагогической диагностики, информации об учебных достижениях и особенностях учебной деятельности в системе открытого образования связана не только с уровнем защиты информационной системы, но и с возможными действиями персонала, который администрирует информационно-коммуникационную педагогическую среду. В традиционной системе образования обучаемый всегда доверяет свои персональные данные преподавателю, однако он лично знает этого преподавателя, общается с ним и имеет возможность убедиться в его высоких морально-этических качествах или выбрать другое учебное заведение. Открытое образование не всегда предполагает личное общение студента и преподавателя, часто общение сводится к обмену сообщениями в виртуальном пространстве, поэтому проблема доверия приобретает новое качество. Преодоление информационной угрозы, связанной с накоплением персональных

данных, результатов педагогической диагностики и мониторинга учебных достижений обучаемых может основываться на четком понимании этой проблемы поставщиком образовательных услуг, осуществлении организационных, воспитательных и информационных мероприятий в педагогическом коллективе и среди технического персонала. С другой стороны, студент может выбирать учебное заведение, осуществляющее дистанционное образование на основании всей доступной информации о качестве образовательных услуг. Целесообразно, чтобы определенная часть учебного процесса осуществлялась в очной форме. Необходимым условием развития качественного образования является обратная связь, широкое информирование общественности относительно особенностей тех или иных педагогических систем.

Будущее образования в обществе знаний неразрывно связано с открытым образованием, которое должно быть совершенным и безопасным. Рассмотренные реальные и потенциальные угрозы информационной безопасности нуждаются в тщательном исследовании с целью поиска эффективных путей их предупреждения и устранения.

Библиографический список

1. Бармен Скотт. Разработка правил информационной безопасности. – М.: Вильямс, 2002. – 208 с.
2. Галатенко В. А. Стандарты информационной безопасности. – М.: Интернет-университет информационных технологий, 2006. – 264 с.
3. Малюк А.А. Теория защиты информации. – М.: Горячая линия - Телеком, 2012. – 184 с.
4. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. – М.: Книжный мир, 2009. – 352 с.
5. Манако А. Ф. К. М. Синица КТ в обучении: взгляд сквозь призму трансформаций // Образовательные Технологии и Общество. - 2012. - Том 15. - № 3. - С. 392-413.

INFORMATION SECURITY IN THE SYSTEM OF EDUCATION

A.A. Kashkaroyeva, *candidate of social sciences, associate professor*

N.E. Atakanova, *lecturer*

**Institute for social development and entrepreneurship
(Kyrgyzstan, Bishkek)**

***Abstract.** Problems of information security in open education systems are discussed from the point of view of the individual, society and state. We consider the potential and real threats to information security and the objects that need protection. We investigate the views of students and teachers on the issues of confidentiality of information in the computer-oriented teaching environment. The approaches to finding ways to prevent and overcome the threats to information security.*

***Keywords:** information security, information and communication technologies, information product, information threats.*