

# Проблемы обеспечения безопасности электронного образования в учебных заведениях

Фирудин Агаев, Гюлара Мамедова

Институт Информационных Технологий НАНА

depart10@iit.ab.az

**Аннотация**— Потребность обучения в виртуальной образовательной среде растёт из года в год. Возрастает число образовательных учреждений, создавших свою информационно-образовательную среду в интернете. В данной статье обсуждаются проблемы обеспечения информационной безопасности в виртуальном образовательном пространстве. Особое внимание уделяется современным педагогическим технологиям как средству обеспечения информационной безопасности обучения в сети.

**Ключевые слова**— электронное образование; безопасность электронного образования; угрозы безопасности; дидактические риски; технологические риски.

## I. ВВЕДЕНИЕ

В современной системе образования электронное образование занимает особое место и активно используется как в учебных заведениях, так в других организациях. Ведущие мировые аналитические компании предсказывают электронному образованию большое будущее. Так, годовой доход e-learning на рынке в ряде стран исчисляется уже в миллиардах [1].

Современные информационные технологии создают благоприятные условия для развития личности. Использование Интернета позволяет учиться и совершенствовать свои знания на протяжении всей жизни. Однако доступность к информационным ресурсам сети также создают определённые проблемы – угрозы зависимости от негативной, противоречивой или агрессивной информации. Это является не только социальной, но и педагогической проблемой.

Национальная безопасность Азербайджана существенным образом зависит от обеспечения информационной безопасности. Под информационной безопасностью понимается состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

В Концепции национальной безопасности Азербайджана [2], утвержденной Указом Президента республики (2007 год), отмечается, что в современных условиях всеобщей информатизации и развития информационных технологий усиливаются угрозы национальной безопасности Азербайджанской Республики в информационной сфере.

## II. ОСНОВНЫЕ ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО ОБРАЗОВАНИЯ

Одним из условий виртуального образования является самостоятельное использование обучаемыми информации из различных источников Интернета. Однако, эта информация порой несет искажённую картину мира и негативно влияет на детей и подростков. В связи с этим необходимо обучить студентов и школьников противодействовать манипулированию их сознанием. Без решения этой проблемы не представляется возможным осуществить полноценное развитие личности.

Большинство ученых и исследователей в мире утверждают, что источниками факторов риска информационной безопасности являются как информационная среда, её ресурсы, так и сам человек, конкретный индивид.

Основными требованиями обеспечения безопасности электронного обучения являются:

- Конфиденциальность (пользователь может получить доступ лишь к тем объектам, к которым ему этот доступ разрешен);
- Целостность (только авторизованные пользователи могут внести изменения в базу данных и программы);
- Обеспечение доступности;

При этом, безопасность системы должна быть обеспечена на уровнях сетевой инфраструктуры, операционной системы и базовых сервисов, приложений и баз данных.

По мнению ученых из Мельбурнского университета К. Грей и С. Томсона[3], можно перечислить следующие типичные угрозы нормальному функционированию системы электронного обучения:

- Неавторизованный доступ к цифровому контенту (кража и модификация данных),
- Нарушение целостности учебных ресурсов,
- Нарушение процедур тестирования обучаемых (проблемы идентификации студентов, списывание, плагиат и неадекватное оценивание знаний студентов),

- Нарушение надежности и бесперебойности работы служб и сервисов учебного заведения.

Рассматривая вопросы безопасности системы электронного обучения, необходимо учитывать все риски и уязвимости такой структуры. Следует отдельно выделить риски дидактической системы электронного образования, связанные, прежде всего, с профессорско-преподавательским составом.

Во-первых – это риски, связанные с компетентностью преподавателей системы. Дидактический риск возникает в том случае, когда преподаватель не обладает нужным уровнем компетентности и не уделяет должного внимания обновлению учебного курса и связан с качеством учебного материала, предлагаемого преподавателем.

Технологический риск возникает вследствие неспособности преподавателей в полной мере использовать современные средства ИКТ, когда преподаватель полностью перекладывает на систему электронного управления учебным процессом ответственность за процедуру аттестации студента.

Во-вторых, это риски, связанные с организацией учебного процесса. Эти риски возникают при неправильном планировании и недостаточном контроле учебного процесса со стороны преподавателей. Некоторые преподаватели, ведущие смежные дисциплины, не информируют друг друга, а на занятиях повторно излагают некоторые элементы курса, не согласовывая отдельные понятия этих дисциплин.

Третья группа рисков возникает непосредственно в ходе учебного процесса в результате неадекватного поведения студентов, низкого уровня профессиональной ответственности преподавателя и нарушения последним трудовой дисциплины.

Четвертая группа рисков связана с низким уровнем подготовки некоторых студентов, вследствие которого они не могут выдерживать заданный преподавателем и электронной системой темп обучения. Поэтому, необходима постоянная мотивация обучаемого. Некоторые студенты ведут себя неадекватно и не могут наладить контакт с преподавателями.

Кроме этого, в деятельности любого учебного заведения возникают риски, связанные с административным персоналом, который в данном случае также может выступать и как объект, и как субъект атаки на систему электронного обучения.

Ученые В.И.Зуев и Е.П.Куркина из «Института социальных и гуманитарных знаний» [4] (Казань), исследуя проблему безопасности электронного обучения, представили ее в виде модели куба, гранями которого являются:

1. Информационная среда – всемирная сеть интернет; сетевая информационная среда учебного заведения; персональная сетевая информационная среда.
2. Программное обеспечение, информационные ресурсы, учебные ресурсы.

3. Человеческие ресурсы – администрация, преподаватели и студенты

Адекватная оценка всех уязвимостей, рисков и угроз системы электронного обучения позволило им создать модель, на основе которой может быть разработана стратегия защиты.



Моделирование угроз является неотъемлемой частью системы безопасности электронного обучения. Внимание к проблеме безопасности на начальном этапе создания защищенной системы электронного обучения позволит осуществить анализ планирования и архитектуры системы с целью обнаружения и устранения проблем защиты уже на уровне проектирования.

Проблемы информационной безопасности школьников и студентов заключаются в совершенствовании умений работать с информацией, в формировании и развитии их критического мышления, что достигается современными педагогическими технологиями как основной составляющей учебного процесса. К этому также следует отнести и умение безопасной работы на компьютере, в Интернете и сети учебного заведения, включая умение работать с антивирусными программами на тестирование объектов компьютера на наличие компьютерных угроз, соблюдение основных требований законодательства Азербайджана в области обеспечения информационной безопасности и лицензионной политики использования программного обеспечения.

Владение современными педагогическими технологиями является одной из составляющих профессиональной компетентности учителя школы, преподавателя вуза и преподавателя дистанционного обучения. Педагогические технологии электронного обучения – это совокупность методов и приёмов обучения, обеспечивающих осуществление учебно-воспитательного процесса дистанционно в соответствии с выбранной концепцией и целями обучения.

Разнообразные виды деятельности, творческие задания, тщательно подобранные ссылки на надёжные источники интернет-ресурсов, а также интерактивные формы общения друг с другом и с преподавателем, способствуют повышению эффективности процесса обучения и защищённости обучаемых от негативной информации сети Интернет.

Одним из условий обеспечения безопасности электронного образования является также и подготовка педагогических кадров, владеющих современными педагогическими и информационными технологиями, организация учебного процесса с учётом особенностей виртуального обучения.

#### ЗАКЛЮЧЕНИЕ

Информационная безопасность виртуального обучения обеспечивается влиянием всех компонентов информационно-образовательной среды электронного образования: целью, задачами, содержанием курса, видами деятельности, педагогическими технологиями, методами, организационными формами, дополнительными источниками, интернет-ресурсами и т.д.

Очевидно, что в агрессивной и неконтролируемой информационной среде наиболее незащищенными становятся обучаемые, у которых еще не сформировано четкое мировоззрение и критическое мышление. В исследованиях Д. Халперна доказано, что критическое мышление можно эффективно формировать, но в авторитарных обществах навыки критической оценки информации сформированы слабее, и граждане таких государств часто подвержены большей внушаемости [5].

Важным способом защиты от нежелательного контента является развитие критического мышления, для чего обучаемый должен научиться:

- правильно искать нужную информацию в Интернете (формулировка ключевых слов, ориентация в перечне результатов поиска);
- правильно оценивать надежность сетевых ресурсов (уметь дифференцировать нужную информацию и информационный шум, выявлять ее качество и регулярное обновление и др.);

При этом необходимо помнить, что основу качества знаний в системе электронного обучения определяют три основных компонента: качество учебно-методических материалов (обучающий контент); профессиональная компетентность преподавателей; качество информационной насыщенности и материально-технической оснащенности образовательной среды.

#### ЛИТЕРАТУРА

- [1] <http://www.elearning-russia.ru>
- [2] Распоряжение Президента Азербайджанской Республики “Об утверждении Концепции национальной безопасности Азербайджанской Республики” 23 мая 2007 года, № 2198.
- [3] K. Gray, C. Thompson, “Students as Web 2.0 authors: Implications for assessment design and conduct,” *Australasian Journal of Educational Technology*, vol. 26, no. 1, pp.105-122, 2010.
- [4] В. И. Зуев, Е. П. Куркина “Риски электронного обучения: модели и метрики,” *Современные технологии и ИТ – образование: VI международная научно-практическая конференция*. М.: ИНТУИТ.РУ, 2011.
- [5] Д. Халперн “Психология критического мышления.” – СПб., 2000.