Казинец Виктор Алексеевич
канд. физ.-мат. наук, доцент, доцент, заведующий кафедрой
ФГБОУ ВО «Тихоокеанский государственный университет»
г. Хабаровск, Хабаровский край

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ ДИСТАНЦИОННОМ ОБУЧЕНИИ

Аннотация*: в статье рассмотрены вопросы информационной безопасности, возникающие в процессе внедрения дистанционного обучения с помощью новых информационных технологий.*

Ключевые слова*: информация, информационная безопасность, информационные технологии, электронное обучение, дистанционное обучение.*

Технологическое усложнение образовательного процесса, переход к электронному обучению неизбежно влечет за собой рост уязвимости системы. Причем, на этом этапе происходит интерференция традиционных рисков системы образования (педагогических, психологических и пр.) с рисками, характерными, в первую очередь для ИТ-сферы. То есть любая система электронного обучения наряду с педагогическими задачами должна решать стандартные задачи по обеспечению информационной безопасности

Напомним, что с точки зрения информационной безопасности, любая информационная система должна обеспечить конфиденциальность целостность и доступность информации. Решение данной задачи поддержано нормативно-правовым модулем, в котором описаны правила поведения в информационном пространстве как субъекта, так и юридического лица. Следует отметить, что данные вопросы рассматриваются на разных уровнях в частности на парламентских слушаниях в совете федераций 24 мая 2017 года на заседании комитета совета федерации по конституционному законодательству и государственному строительству рассматривался вопрос «Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве».

Участники парламентских слушаний уделили большое внимание обеспечению безопасности и развития детей в информационном пространстве, При этом они констатировали, что в настоящее время дистанционное образование на основе информационных технологий недостаточно поддержано на законодательном уровне и поручили Министерству Образования и Науки РФ в короткие сроки рассмотреть этот вопрос. Заметим, как показали опросы учителей и студентов, многие из них недостаточно знакомы с законодательством определяющем нашу жизнь в информационном пространстве. Кроме этого, были выделены вопросы, решение которых необходимо при организации дистанционного обучения, а именно:

Отсутствие регламентации и ненадлежащая организация защиты детей от противоправного контента в образовательных организациях, нехватка в них компетентных специалистов в области информационной безопасности;

Отсутствие должного контроля за соблюдением законодательства владельцами сайтов, провайдерами хостинга и операторами связи, оказывающими услуги по предоставлению доступа к сети Интернет;

Отсутствие системы мер по противодействию распространения материалов экстремистской направленности, пропаганде молодежных суицидов в социальных сетях;

Нехватка развивающего и обучающего контента в сети Интернет, интересного детям, а также его пропаганды.

Хотелось бы обратить внимание педагогов, участвующих в работе дистанционного обучения на то, что мы с вами часто нарушаем закон о персональных данных, закон об авторском праве, достаточно часто отступаем от образовательного стандарта, необоснованно используем гипертекстовую и мультимедийную технологию и неактуальную информацию. Целесообразно работающим и обеспечивающим дистанционное обучение ознакомиться со следующим законами:

1. «О персональных данных».

2. «О защите детей от информации, причиняющей вред их здоровью и развитию».

3. «Об авторском праве и смежных правах».

Важную роль в обеспечении информационной безопасности играет программно-технический модуль, работа которого регламентируется соответствующими ГОСТами. При организации дистанционного обучения необходимо решить ряд задач на уровне сетевой инфраструктуры, на уровне операционной системы и базовых сервисов, на уровне приложений, на уровне баз данных, что требует привлечения квалифицированных специалистов (решение этих задач самостоятельно возможно, но как показывает практика, приводит к большим сложностям, в дальнейшем).

Нужно помнить, что программно-технический модуль должен нам обеспечить защиту от распространения вирусов, спама, программных ловушек, несанкционированного доступа, хищений информации, разрушения аппаратуры, должен учесть слабость и незащищенность интернет каналов.

Дистанционное обучение требует определенного уровня владения информационными технологиями преподавателем, позволяющим ему использовать их в своей профессиональной деятельности и, хотя бы уметь поддерживать разговор с «продвинутыми» учениками на данную тему.

То есть необходимо непрерывная переподготовка преподавателей в области использования информационных технологий в дистанционном обучении.

Если нормативно-правовой модуль и программно-технический это забота соответствующих специалистов, а наша задача правильно использовать результаты их работы, то контент, взаимодействие с обучающимися, социальные сети, организация работы в среде электронного обучения непосредственно касается нас с вами (преподавателей, учителей, организаторов и руководителей образовательного процесса).

Переход на дистанционное обучение фактически всем педагогическим сообществом, вызванный объективными обстоятельствами, достаточно точно определил состояние образовательной среды:

1) недостаточный уровень подготовки преподавателей в области использования информационных технологий в профессиональной деятельности;

2) фактически отсутствие подготовки педагогов в области информационной безопасности;

3) неготовность педагогов использовать новые формы и методики обучения присущие дистанционному обучения;

4) «информационное загрязнение», недостоверность, неактуальность информации.

Системы электронного обучения во многих образовательных учреждениях находятся на стадии создания и использует те материалы и возможности, открывшие свои электронные образовательные ресурсы. Для построения системы информационной защиты необходимо иметь некоторую модель электронного учебного заведения и выбрать базовые параметры, определяющие содержание и организацию информационной безопасности.

При построении системы электронного обучения целесообразно учитывать специфику данного обучения. Дистанционная образовательная среда предполагает активное участие учащихся и учителей в создании и наполнении баз учебных материалов, новые формы взаимодействия между учениками и учителями, большое число контента по заданной теме (этот контент никем не рецензирован и часто несет искаженную информацию), предполагает объединение разнородных потоков информации, сочетает как известные, так и новые формы обучения, следует помнить про использование социальных сервисов и социальных сетей.

Традиционный подход к рассмотрению безопасности электронного обучения включает в себя следующие компоненты [6]:

1) информационная безопасность электронного обучения;

2) психологическая безопасность электронного обучения;

3) дидактическая безопасность электронного обучения;

4) физическая безопасность электронного обучения.

Нас в первую очередь интересует информационная безопасность электронного обучения, она предполагает заполнение учебного пространства верифицированными мультимедийными ресурсами, организацию работы с ними обучающихся и педагогов, организацию учебной траектории учащегося, возможность интерактивного взаимодействия педагога и ученика и регламентация доступа участников образовательного процесса к электронной образовательной системе, защиту персональных данных обучаемого.

Все вышеперечисленное являются объектами атак взломов возможно подвергаются искажениям или уничтожению, при этом возникают вопросы связанные с авторскими правами преподавательского состава размещенные в сети, с плагиатом, защитой целостности информационных ресурсов, с управлением образовательным процессом и т. д.

Опыт работы в электронно-образовательной среде показывает, что наиболее часто мы сталкиваемся с несанкционированным доступом к контенту, часто к серверам с неадекватностью учебных ресурсов (они часто берутся в интернете), с нарушением процедур сдачи экзаменов, списывания плагиата, с нарушениями законодательства.

Наконец, информационные технологии являются базисом, на основе которого строится новая система коммуникаций с высоким уровнем интерактивности, напоминающем разговор двух лиц, новые медиа могут быть индивидуальными до такой степени, чтобы донести специальное сообщение до каждого человека внутри огромной аудитории. При этом новые коммуникационные технологии также асинхронны, что означает их способность отправлять или получать сообщения в удобное для конкретного человека время, все это позволяет влиять на состояние политической, экономической и оборонной безопасности России.

В наше время существенное внимание уделяется вопросам моделирования управления в социальных сетях, построенные модели позволяют построить систему управления участниками социальных сетей, формирования у них нужного взгляда на те или иные события и явления. В связи с вышеизложенным целе-

сообразно в учебные планы педагогических институтов и университетов ввести курс «Информационная безопасность» в рамках которого необходимо рассмотреть следующие модули:

1. Нормативно-правовой модуль, содержащий те законы, которые применяются и используются в обыденной жизни в современном информационном обществе с примерами их применения.

2. Административный модуль, отражающий правила и нормы поведения гражданина во время работы в организации или учреждении с современными информационными системами.

3. Программно-технический модуль, в рамках которого необходимо ознакомить обучаемых с современными программно-техническими средствами обеспечивающих информационную безопасность пользователя.

4. Социальные сети, модели управления в социальных сетях.

Список литературы

1. Зуев В.И. Безопасность электронного обучения // Совершенствование подготовки IT-специалистов по направлению «Прикладная информатика» для инновационной экономики: сборник научных трудов. – М., 2010. – С. 81–85.

2. Зуев В.И. Безопасность электронного обучения / В.И. Зуев, В.П. Чирко // Сборник тезисов докладов XII конференции представителей региональных научно-образовательных сетей “Relarn-2010”. – Н. Новгород, 2010.

3. Привалов А.Н. Основные угрозы информационной безопасности субъектов образовательного процесса / А.Н. Привалов, Ю.И. Богатырева // Известия ТулГУ. Гуманитарные науки. – Тула, 2012. – Вып. 3. – С. 427–431.

4. Тимошенко В.Н. Вакцинация от фальсификации / В.Н. Тимошенко, М.И. Романова, В.А. Казинец [и др.]. – Хабаровск, 2016. – 95 с.

5. Федеральный закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».

6. Федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных».

7. Федеральный закон от 29.12.2010 г. №438-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (редакция от 29.06.2015 г.).

8. Howard, M. (2003). Fending off Future Attacks by Reducing Attack Surface. URL: http://msdn.microsoft.com/en-us/library/ms972812 (access date: 09.01.19).

9. IBM Lotus Workplace Collaborative Learning (LWCL). URL: http://e-college.ru/elearning/lwcl/ (access date: 09.11.2019).