

УДК 374.1:004

Латагуз М.М., старший преподаватель
Хамянок В.П., ассистент

Кузбасский государственный технический университет имени Т.Ф. Горбачёва

Latguz M.M., Senior Lecturer
Hamyanok V.P. assistant
T.F. Gorbachev Kuzbass State Technical University

БЕЗОПАСНОСТЬ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПРИ ИСПОЛЬЗОВАНИИ ЦИФРОВЫХ ТЕХНОЛОГИЙ

SAFETY OF THE EDUCATIONAL PROCESS WHEN USING DIGITAL TECHNOLOGIES

Современное образование, идя в ногу со временем, видоизменяется и подчиняется требованиям рыночных отношений. Образовательный процесс наполняется цифровыми технологиями. В каждом образовательном учреждении имеется своя образовательная платформа или для взаимодействия преподавателя и обучающегося используются одновременно несколько. Для более эффективной мобильности процесса задействованы не только компьютеры, планшеты и смартфоны, разнообразили его. Цифровые технологии позволяют работать удаленно, получать новые знания в дистанционном формате. Рынок труда в настоящее время не заинтересован в моноспециалистах, имеющих один уровень подготовки и компетенций. Индустрия и бизнес ждут специалистов, которые имеют опыт работы в реальных проектах. Специалистов, связанных с реальным миром, которые получая новые знания умеют их интерпретировать, мобильных, способных самостоятельно принимать решение.

Высшая школа набирает темпы перехода от традиционных к развивающим образовательным технологиям. Задача вуза не просто подготовить выпускника нужной специализации, а специалиста, который уже на начальном этапе обучения вольётся в работу реальных проектов предприятий, социальных проектов города и т.п. В образовательных вузах России начинает приживаться новая модель образования – проектное обучение. Проектное обучение – динамическая модель востребованных компетенций. Если коротко о технологии эта тесная связь с различными специалистами, преподавателями, которые могут вести диалог и консультации в онлайн режиме. В настоящее время многие вузы страны и мира привлекают в процесс образования производственников, индивидуальных предпринимателей, экспертов, иностранных специалистов. А участники проектного обучения могут общаться с участниками проекта по видеосвязи, решать про-

блемные вопросы проекта на различных интернет платформах, которые позволяют планировать, анализировать, выполнять графические элементы и презентации, обращаться к нормативным и литературным источникам различных интернет ресурсов.

В свою очередь преподаватель или руководитель проекта может удаленно контролировать процесс выполнения работы над проектом и контролировать работу каждого участника в отдельности. Автоматически в режиме реального времени выполнить анализ цифрового следа выполняемой работы. В процессе обучения студенты получают, дополнительные знания, умения и навыки. Современный вуз, использующий цифровые технологии и цифровые образовательные ресурсы: виртуальные лаборатории, обучающие материалы с использованием технологий виртуальной реальности, тренажеры, симуляторы. Обучающиеся имеют свободный доступ к единой цифровой среде. А теперь ещё к этому добавить различные онлайн – курсы. Привлечение сторонних экспертов, проведение международных конференций.

Понятно, что вся информация цифровых технологий не может храниться на собственных серверах. Использование облачных технологий в образовательном процессе очевидно.

«Облачное хранилище данных (англ. Cloud storage) — модель онлайн-хранилища, в котором данные хранятся на многочисленных распределённых в сети серверах, предоставляемых в пользование клиентам, в основном, третьей стороной. Данные хранятся и обрабатываются в так называемом «облаке», которое представляет собой, с точки зрения клиента, один большой виртуальный сервер. Физически же такие серверы могут располагаться удалённо друг от друга географически» [1]

Облачными хранилищами являются такие интернет-сервисы, как: Dropbox, OneDrive, Google Drive, iCloud, Яндекс.Диск, Облако Mail.Ru, Mega, BOX, pCloud, Files.fm, WDfiles.ru, wdho.ru, Anonfile.com My-Files.R это всего лишь крупные, практически у всех на слуху. Да, использование хранилищ имеет преимущества.

Вот только несколько преимуществ облачных технологий:

- ✓ Виртуальные сервисы освобождают от необходимости работать с флэш-накопителями и решают проблему по ограничениям объема на жестком диске – пользователю дается несколько гигабайт бесплатно, а при необходимости их можно докупить.
- ✓ Не нужно покупать лицензионное программное обеспечение. Облачные технологии позволяют экономить на приобретении, поддержке, модернизации ПО и оборудования.
- ✓ Сервис позволяет одновременно работать с одним файлом нескольким сотрудникам или творческой группе.

- ✓ Пользователь может хранить информацию в любом формате и свободно получать к ней доступ с любого устройства – привязки к памяти конкретного компьютера нет.
- ✓ Их можно использовать на разных платформах, а при необходимости – масштабировать. Эластичная и гибкая структура позволяет это легко сделать.

Как прекрасно не представлена возможность цифровых технологий в образовательном процессе высшего или иного уровня образования. Необходимо озвучить и условия безопасности, поддержание высокого уровня информационной безопасности.

Информационная безопасность (англ. Information Security, а также — англ. InfoSec) — практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная или, например, физическая). Это состояние защищенности информационных ресурсов (информационной среды) от внутренних и внешних угроз, способных нанести ущерб интересам личности, образовательного процесса, государства (национальным интересам).

Безопасность информации — защищенность информации от нежелательного ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Информационная безопасность в образовательном процессе имеет свои особенности. К угрозам намеренного или ненамеренного воздействия могут подвергаться следующие объекты:

компьютерное и другое оборудование образовательной организации, в отношении которого возможны воздействия вредоносного программного обеспечения, физические и другие воздействия;

программное обеспечение, применяемое в учебном процессе или для работы системы;

данные, которые хранятся на жестких дисках или портативных носителях;

обучающиеся, которые могут подвергаться стороннему информационному воздействию;

персонал, поддерживающий работу ИТ-системы.

Угрозы информационной безопасности образовательного учреждения могут носить непреднамеренный и преднамеренный характер.

К непреднамеренным угрозам можно отнести все аварийные ситуации локального и территориального характера, программные сбои, ошибки антропогенного характера, сбои всех систем связи. Такие угрозы имеют временное воздействие. И достаточно быстро устраняются.

Намного более опасными являются угрозы информационной безопасности намеренного характера. Такие угрозы могут исходить от любых субъектов: хакеры, конкуренты, обучающиеся и лиц входящих в их окружение, персонала организации. Преднамеренное воздействие на компьютерные системы или программное обеспечение, удаленные сети и хранилища. Злоумышленники могут достаточно легко нарушать связи между такими удаленными компонентами, что полностью выводит систему из строя.

Если подробно перечислять все цифровые переплетения и взаимодействия, которые требуют цифровой и информационной безопасности. То перед нами предстанет айсберг.

Законодательная база для безопасности цифрового образовательного процесса должна быть основой для создания внутренних локальных нормативных документов.

Приказ Министерства образования и науки РФ от 5 апреля 2017 г. № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры».

Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг. обусловлена только основными направлениями.

Необходимо в каждом образовательном учреждении рассматривать все риски и источники угроз, уязвимости. А сам процесс цифрового образования сопровождает команда профессионалов, которые эффективно управляют рисками в области технических мер защиты информации, юридической ответственности, а также стандартов обучения пользователей и администраторов.

Список литературы

1. Баева Л.В. Проблемы и перспективы развития открытого дистанционного образования в условиях электронной культуры // Информационное общество. 2017. №3. 48-59.
2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.06. № 149-ФЗ;
3. Николенко, В.Ю. Базовый курс системной инженерии: учебное пособие / В. Ю. Николенко. – М.: МФТИ, 2016 -290 с.
4. https://ru.wikipedia.org/wiki/Облачное_хранилище_данных

References

1. Baeva L.V. Problems and prospects for the development of open distance education in the context of electronic culture // Information Society. 2017. № 3. 48-59p.
2. Federal Law "On Information, Information Technologies and Information Protection" dated 27.07.06. № 149-FZ;
3. Nikolenko V.Y. Basic course of systems engineering: textbook. Nikolenko V. Y. - M.: MFTI, 2016 -290 p
4. <https://ru.wikipedia.org/wiki/cloud data storage>