(cc) BY

Гудков Владимир Владимирович

магистрант

Брянский филиал ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации»

г. Брянск, Брянская область

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В СИСТЕМЕ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

Аннотация*: в статье рассмотрены основные проблемы информационной безопасности в деятельности дистанционного обучения в образовательных организациях, а также при обучении в коммерческом предприятии. Описаны основные методы для защиты персональных данных в организациях: нормативно-правовые, морально-этические, административно-организационные, физические, технические.*

Ключевые слова*: информационная безопасность, образовательное учреждение, дистанционное обучение.*

Деятельность образовательного процесса должна соответствовать многим нормам и требованиям, одним из которых является обеспечение высокого уровня информационной безопасности (ИБ). Однако ИБ в рамках образовательного процесса не ограничивается только сохранением личных данных обучающихся, важной задачей выступает ограждение пользователей от различного рода пропаганды и противоправных действий.

На основе изложенных данных было сформулировано определение ИБ – это комплекс мер различного характера, направленных на реализацию двух основных целей: защиты персональных данных от вмешательства и хищения информации и защиты учащихся от рекламы и пропаганды, запрещенной законом информации.

Законодательство РФ предусматривает защиту персональных данных в трех направлениях [2]:

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

1) персональные данные и сведения, которые имеют отношения к учащимся, преподавательскому составу, персоналу организации, оцифрованные архивные документы;

2) обучающие программы, базы данных, библиотеки, другая структурированная информация, применяемая для обеспечения учебного процесса;

3) защищенная законом интеллектуальная собственность.

Поэтому ответственные лица, управляющие ИБ в организации, должны иметь соответствующий опыт и квалификацию в данной области. Обусловлено это тем, что они выполняют важные функции в отношении информационный безопасности: обеспечивают сохранность данных и их доступность авторизованным лицам, а также осуществляют поддержание конфиденциальности сохраняемых данных и предотвращают к ним доступ третьими лицами.

Однако, набирающая популярность в последнее время тенденция к дистанционному обучению, существенно влияет на требования к обеспечению защиты информации. Связано это с тем, что при дистанционном обучении используется широкое множество различного программного обеспечения и информационных технологий. Данные аспекты накладывают новые требования в области передачи данных в этих системах.

Дистанционное обучение нашло распространение не только в образовательных учреждениях, но и в рамках коммерческих компаний с целью подготовки кадров в интересующей сфере без отрыва от производства. Особенно актуальна эта тема для крупных промышленных предприятий, имеющих большое количество филиалов по всей стране.

В настоящее время дистанционное обучение проходит с помощью интернет-ресурсов. Это могут быть сайты с лекциями и практическими занятиями, вебинарами и тестами, а также сервисы, в общем виде называемые «e-learning». В последнее время распространено также обучение с помощью мобильных технологий «m-learning». По сути, это ответвление электронного образование, ставшее популярным благодаря использованию большого количества средств мобильной связи.

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

Для осуществления деятельности дистанционного обучения в основном используются следующие виды средств организации [1]:

1) LMS – Learning Management Systems – системы управления обучением, или же системы дистанционного обучения;

2) LCMS – Learning Content Management Systems – системы управления учебным контентом;

3) инструменты для организации и проведения вебинаров, виртуальных классов, онлайн-конференций;

4) средства для разработки электронных курсов и учебного контента;

5) SaaS-сервисы.

Во всех описанных системах актуальны три основные аспекта: доступность информации, конфиденциальность информации и ее целостность.

Чтобы выполнить данные требования в отношении безопасности существуют различные способы защиты: нормативно-правовой, морально-этический, административно-организационный, физический, технический.

Нормативно-правовой способ заключается в обеспечении безопасности данных с помощью нормативных документов, Трудового и Гражданского кодекса, ФЗ «Об информации».

Со стороны морально-этического вопроса, для обеспечения безопасности создается список различных сайтов и документов, которые могут нанести вред психическому состоянию человека. В дальнейшем, доступ к этим источникам блокируется в рамках образовательного процесса.

Административно-организационные меры подразумевают под собой разработку различного рода документации (методики, инструкции, должностные инструкции, регламенты и т. п.), которые будут предписывать определенный порядок использования обучающих программ.

Под физическими мерами понимаются такие действия, которые ограничивали доступ к информации со стороны третьих лиц. Например, самым простым способом является аутентификация пользователя. Также, к данным мерам можно

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

отнести создание правил копирования важной информации и правил по созданию паролей.

Технические меры защиты подразумевают под собой использование специального программного обеспечения, например DLP и SIEM-системы. Данные системы вовремя обнаруживают возможные взломы и атаки, которые угрожают ИБ.

Но стоит помнить, что на безопасность дистанционного обучения влияет не только используемое программное обеспечение, а также и люди, цели, регламенты, различные средства. Необходимо учитывать все факторы угроз, чтобы информационная безопасность соблюдалась на высшем уровне.

Список литературы

1. Струбалин П.В. Информационные технологии, обеспечивающие работу и безопасность систем электронного дистанционного обучения / П.В. Струбалин, Н.Б. Фролова // Информационная безопасность регионов. – 2015. – №4 (21). – С. 12–18.

2. Информационная безопасность в образовательной организации [Электронный ресурс]. – Режим доступа: https://www.smart-soft.ru/blog/informatsionnaja_bezopasnost_v_obrazovateljnoj_organizatsii/ (дата посещения 20.04.2021).

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)