Кушнир Светлана Ивановна
канд. ист. наук, доцент, доцент
ФКОУ ВО «Воронежский институт
Федеральной службы исполнения наказаний»
г. Воронеж, Воронежская область
Кушнир Михаил Станиславович
студент
ФГБОУ ВО «Воронежский государственный университет
инженерных технологий»
г. Воронеж, Воронежская область

ЦИФРОВОЕ ОБРАЗОВАНИЕ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Аннотация*: цифровое образование является одним из приоритетных направлений в современной методике обучения. Однако существует опасность потери данных участников образовательного процесса, попадания таких данных в руки мошенников, и незаконное их использование в дальнейшем. Поэтому необходимо проанализировать такие компоненты информационной безопасности, как конфиденциальность, целостность, доступность, аутентификация и авторизация, защита от вредоносных программ, аудит и мониторинг и даже – физическая безопасность.*

Ключевые слова*: цифровое образование, информационная безопасность, конфиденциальность, правильность, целостность, доступность.*

Цифровое образование является одним из важных направлений в сфере современного образования. Проект в области образования «Современная цифровая образовательная среда в Российской Федерации» был утвержден Правительством Российской Федерации 25 октября 2016 г. в целях реализации государственной программы «Развитие образования» [1, С. 74]

К 2025 году планируется задействовать в цифровом обучении около 11 млн. человек. Однако, при всей амбициозности проекта, следует учесть такую важную составляющую, как информационная безопасность, которая включает в се-

бя следующие компоненты: конфиденциальность, целостность, доступность, аутентификацию и авторизацию, аудит и мониторинг, защиту от вредоносных программ, в конце концов – физическую безопасность [2]

Рассмотрим и проанализируем некоторые из них.

Конфиденциальность. Согласно статье №2 Федерального закона «Об информации, информационных технологиях и защите информации», конфиденциальность – «обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя» [3]

Обеспечение конфиденциальности включает процедуры и меры, предотвращающие раскрытие информации нелегитимным пользователям. К такой информации относятся имя, фамилия, дата рождения, паспортные данные, адрес проживания и регистрации и некоторые другие личные данные, которые могут быть затребованы учебным заведением. Такими данными могут воспользоваться злоумышленники в преступных целях.

Опираясь на вышесказанное, можно сделать вывод, что система цифрового обучения должна всеми возможными способами обеспечивать конфиденциальность обрабатываемых сведений, в том числе согласно действующему законодательству в области защиты персональных данных [1].

Информационная безопасность также включает такие аспекты, как целостность, правильность, неискаженность и неизменность данных. Цифровая образовательная система должна обеспечивать, чтобы данные не подвергались изменениям и ошибкам при их передаче, хранении или отображении.

В контексте цифровой образовательной системы, сервис информационной безопасности не менее важен, чем конфиденциальность, поскольку:

1) изменение и искажение образовательного контента недопустимы, за исключением случаев, когда преподаватели или администраторы системы вносят легитимные изменения для уточнения или исправления ошибок, а также обновления в соответствии с образовательными стандартами или законодательством;

2) Образовательный контент должен соответствовать нормативно-правовым требованиям и быть идентичным эталону, расхождения и приближенные данные не допустимы;

3) критически важно, чтобы структура образовательного контента и самой цифровой образовательной среды не содержала логических ошибок. Нарушения в логике работы платформы могут привести к техническим проблемам, недоступности материалов или разделов среды.

Основными методами обеспечения целостности информации при хранении в информационных системах (в качестве которых выступает ЦОС) являются следующие.

1) резервирование, дублирование и зеркалирование оборудования и данных для обеспечения отказоустойчивости. Например, создание копии образовательной платформы для временного или постоянного переноса образовательного процесса в случае нарушения работы основной системы;

2) резервное копирование и электронное архивирование информации для возможности безопасного восстановления данных. Хранение резервных копий в отдельных хранилищах, не связанных с основной системой;

3) использование средств криптографической защиты (шифрование, хеширование, электронная цифровая подпись) для безопасной передачи данных и обнаружения повреждений. Например, при изменении контента учебного курса использование вышеуказанных средств для обнаружения повреждения данных и предотвращения внесения изменений в существующую систему.

Доступность информации означает состояние, при котором субъекты с правами доступа могут свободно использовать информацию и ресурсы автоматизированной информационной системы. К таким правам относятся чтение, изменение, хранение, копирование и уничтожение информации, а также изменение, использование и уничтожение информационных ресурсов.

Нарушение доступности может происходить, например, через чрезмерную загрузку системы (ddos-атака), внедрение вредоносного кода или в результате стихийных бедствий. Согласно статистике, эти источники угроз составляют

около 13% потерь информационных систем, включая ЦОС. Техногенные угрозы (пожары, проблемы с электропитанием и т. д.) также встречаются примерно в два раза чаще.

Гарантирование доступности цифровой образовательной среды является важной задачей, так как любое временное препятствие в доступе к образовательному контенту нарушает основной принцип обучения – доступность обучения. Кроме того, угроза доступности может повлиять на целостность образовательного процесса, который включает в себя четыре взаимосвязанных компонента: освоение и создание образовательного материала, взаимодействие между учителями и учениками, взаимодействие между педагогами и учениками, а также самостоятельное усвоение материала учащимися. Любое отсутствие этих элементов ведет к существенному снижению эффективности образовательного процесса и обучения. Основными методами обеспечения доступности данных при хранении в автоматизированных системах является использование систем бесперебойного электропитания оборудования, а также резервирование и дублирование вычислительных мощностей, чтобы своевременно восстановить работу системы в случае возникновения угроз.

Цифровая образовательная среда должна быть безопасной по нескольким причинам:

1) защита данных – В цифровой образовательной среде обычно хранится множество личных данных, как учащихся, так и преподавателей. Безопасность данных очень важна для предотвращения несанкционированного доступа и потенциальной кражи личной информации;

2) защита от кибербуллинга – Кибербуллинг, или межличностное насилие в сети, может быть распространено через цифровые платформы образования. Наличие безопасной среды позволяет предупредить и предотвратить случаи кибербуллинга, а также обеспечить безопасное общение между учащимися и преподавателями;

3) защита от вредоносного контента – В цифровой среде могут присутствовать содержимое и платформы, которые могут быть вредными или неподходя-

щими для обучения и развития учащихся. Безопасная среда обеспечивает контроль и фильтрацию такого контента, чтобы предотвратить его попадание в руки детей и дать им возможность учиться в безопасной и подходящей среде;

4) защита от кибератак – Цифровые платформы образования могут быть подвержены кибератакам, которые могут нарушить образовательный процесс и уклониться его цели. Безопасная среда предоставляет механизмы защиты от кибератак и обеспечивает непрерывность обучения.

В целом, безопасная цифровая образовательная среда не только защищает данные и личную информацию учащихся и преподавателей, но и обеспечивает безопасное обучение и развитие учащихся. Это позволяет им чувствовать себя комфортно и защищенными в онлайн-пространстве, что способствует их успешному обучению.

Список литературы

1. Ажмухамедов И.М. Информационная безопасность в цифровой образовательной среде: анализ информационных рисков и выработка стратегий защиты школьников от негативных последствий цифровизации образования / И.М. Ажмухамедов, В.Ю. Кузнецова // Прикаспийский журнал: управление и высокие технологии. – 2020. – №3(51). – С. 74–83. EDN ZZXXGU

2. Кушнир С.И. Шифрование и защита от DDOS-атак как один из компонентов информационной безопасности / С.И. Кушнир, М.С. Кушнир // Инженерное образование в условиях цифоровизации общества и экономики: материалы Всероссийской научно-практической конференции с международным участием. – Чебоксары, 2023. – С. 15–18. EDN FTBYVA

3. Об информации, информационных технологиях и о защите информации: Федеральный закон №149-ФЗ от 27 июля 2006 г.: принят Государственной Думой 8 июля 2006 г. // Собрание законодательства Российской Федерации. – 2006.