УДК 37.013.2

Е. Н. Костров
E. N. Kostrov

ЦЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНЫХ РЕСУРСОВ

GOALS OF INFORMATION SECURITY OF EDUCATIONAL RESOURCES

Аннотация. Доступность образовательных ресурсов, ставшая возможной благодаря повсеместному распространению цифровых технологий, не только открывает новые возможности для обучения и развития, но и существенно повышает угрозы, связанные с информационной безопасностью. В статье характеризуются цели обеспечения информационной безопасности образовательных ресурсов. Для снижения рисков необходимо последовательное применение технических, организационных и правовых мер – именно такой комплексный подход позволит сделать процесс обучения в цифровой среде более безопасным и эффективным.

Abstract. The availability of educational resources, made possible by the ubiquity of digital technologies, not only opens up new opportunities for learning and personal growth, but also significantly increases the threats associated with information security. The article characterizes the goals of ensuring the information security of educational resources. To reduce risks, it is necessary to consistently apply technical, organizational and legal measures – it is this integrated approach that will make the learning process in the digital environment safer and more efficient.

Ключевые слова: информационная безопасность, образование, образовательные ресурсы, кибербезопасность.

Keywords: information security, education, educational resources, cybersecurity.

Доступность образовательных ресурсов, ставшая возможной благодаря распространению цифровых технологий, не только открывает новые возможности для обучения и личностного роста, но и существенно повышает угрозы, связанные с информационной безопасностью. Вопросы её обеспечения являются теперь приоритетными практически для любой организации, ведущей образовательную деятельность, будь то школа, университет или частный образовательный центр [2]. В этой связи очень важно обозначить цели информационной безопасности электронных образовательных ресурсов.

Главная цель – это *защита конфиденциальности данных.* Образовательные учреждения хранят огромные массивы информации об учащихся и преподавателях, других участниках образовательного процесса (персональные данные, академическая успеваемость, финансовые сведения, иная чувствительная информация). Основная задача – не допустить несанкционированный доступ к этим данным, предотвратить их незаконное использование и раскрытие третьими лицами. Для этого необходимо контролировать доступ к информационным системам, применять шифрование данных, использовать авторизацию и аутентификацию пользователей, устанавливать защищённые сетевые соединения. Главным нормативно-правовым документом, которым следует руководствоваться в области защиты данных, является Федеральный закон «О персональных данных» [1].

Другая важная цель – *предотвращение кибератак.* Киберпреступники стремятся получить доступ к конфиденциальным данным для последующего вымогательства и шантажа. Сколько уже в последнее время было случаев, когда преподаватели и научные сотрудники поддавались давлению преступников и отдавали им свои кровные деньги [5]. Кибератаки также могут быть нацелены на срыв учебного процесса, на внесение хаоса и сумятицы в повседневную жизнь. Действенными способами защиты от кибератак служат антивирусные программы, межсетевые экраны и системы обнаружения вторжений. Важно регулярно проводить аудит безопасности, а ещё важнее – повышать уровень цифровой и юридической грамотности, чтобы преподаватели и учащиеся могли самостоятельно противостоять фишинговым атакам и разнообразным уловкам социальной инженерии [6].

Третья значимая цель информационной безопасности – *обеспечение доступности и непрерывности образовательного процесса.* В случае сбоя информационных систем образовательное учреждение может столкнуться с проблемой доступа к учебным материалам, онлайн-курсам и другим образовательным ресурсам [3]. В результате может произойти серьёзный срыв

учебного процесса, хотя бы и кратковременный. Избежать этого помогут резервные копии ключевых систем и резервное копирование данных. Для предотвращение подобных случаев необходимо заранее разработать план контингенции.[1] Целесообразно иметь специальные системы мониторинга, позволяющие оперативно устранять проблемы доступности и непрерывности обучения в онлайн и офлайн-формате [4].

Итак, цели информационной безопасности образовательных ресурсов охватывают защиту конфиденциальности данных, предотвращение кибератак и обеспечение доступности и непрерывности образовательного процесса. Достижение этих целей требует комплексного подхода, включающего технические, организационные и правовые меры. Руководство образовательных учреждений должно в текущих условиях чётко понимать всю важность вопросов информационной безопасности и непрерывно развивать соответствующие меры защиты, чтобы обеспечить эффективное обучение студентов и безопасную работу преподавателей.

Список источников и литературы

1. Федеральный закон «О персональных данных» от 27 июля 2006 г., № 152-ФЗ (последняя редакция, с изменениями от 8 августа 2024 г.). Источник: правовая система «КонсультантПлюс» [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 01.08.2023).

2. *Бочаров М.И., Козлов О.А., Симонова И.В.* Анализ современной подготовки педагогических кадров в области информационной безопасности // Инновации на основе информационных и коммуникационных технологий. – 2012. – № 1. – С. 29-32.

3. *Роберт И.В.* Перспективные научные исследования, определяющие развитие информатизации образования // Педагогическое образование в России. – 2014. – № 4. – С. 199-204.

4. *Дубова Ю.С.* Информационная безопасность в киберпространстве // Вестник Киргизско-Российского славянского университета. – 2016. – Том XVI. – № 4. – С.154-157.

[1] Контингенция (от лат. *contingentia* – случайность, непредвиденные обстоятельства) – вероятность наступления какого-либо негативного события в будущем. План контингенции подразумевает подготовку специальных мер, которые позволят пережить это событие с наименьшими потерями [7]. – *Прим. Ред.*

5. *Кормильцева Марина.* Трое преподавателей МГУ и РУДН лишились 35 млн. рублей, поверив мошенникам. Источник: «Газета.Ру». – 2024, 31 августа [Электронный ресурс]. – Режим доступа: https://www.gazeta.ru/social/news/2024/08/31/23819965.shtml (дата обращения: 01.08.2023).

6. *Олейник А.С., Герасимов В.М., Халилуллин Ф.Н., Гайнулова Ю.М., Калинин Д.С.* Технология обеспечения информационной и кибербезопасности в учреждениях высшего образования // Управление образованием: теория и практика (Education Management Review). – 2022. – Том XII. – № 5. – С. 240-247. DOI: 10.25726/v6109-4146-3543-s.

7. *Kenton Will.* What Are Contingencies and Contingency Plans? Definition and Examples. Source: «Investopedia» [e-Source]. – URL: https://www.investopedia.com/terms/c/contingency.asp (accessed: 01.08.2023).